ORDER

1600.54B

ACM-1

OK

FAA AUTOMATED INFORMATION SYSTEMS SECURITY HANDBOOK

February 7, 1989

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

Distribution: A-WXYZE-2; A-FOF-O (LTD)

Initiated By: ACS-300

RECORD OF CHANGES

DIRECTIVE NO.

CHANGE TO BASIC	SUPPLEMENT			OPTIONAL	CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL

FOREWORD

This order establishes comprehensive security policies and standards for all Automated Information Systems (AIS) within the Federal Aviation Administration (FAA), and the facilities housing such systems. Additionally, it applies to office automation, personal computers, word processors, and administrative record keeping systems operated within the FAA jurisdiction. In the context of this order, the term "security" addresses the varying but related concerns of physical asset protection, access control for communications and data base/application resources, accuracy and integrity of data, preservation of personal privacy, and assuring the operational reliability of essential administrative and air traffic control (ATC) computer systems.

This order also establishes risk management program objectives, assigns responsibilities, and provides detailed guidance for conducting risk analyses of FAA AIS, applications, and facilities.

It is intended that this order will provide AIS facility managers, system administrators, designers, planners, and security officers with the necessary guidance that will facilitate effective implementation and application of the provisions of this order.

This order was developed through a coordinated effort of the associate administrators of the Federal Aviation Administration. It shall be used by all FAA personnel in the joint administration of the AIS security program.

T Allan McArtor

T. Allan McArtor
Administrator

TABLE OF CONTENTS

Page No.

Page No.

CHAPTER 1. INTRODUCTION

1. PURPOSE. This order establishes an Automated Information Systems (AIS) Security Program, formerly known as Automatic Data Processing (ADP) Security Program. This order designates program objectives, establishes an AIS Security Organization, assigns responsibilities, and provides detailed guidance to ensure that an appropriate level of AIS security is implemented throughout the FAA data processing activities. It implements Order DOT 1640.7, Department of Transportation Automatic Data Processing Security Policy, and Order DOT 1640.8, Department of Transportation Automatic Data Processing Security. This order also implements within FAA, and adapts to the FAA Automatic Information Systems environment, the guidance set forth in National Security Decision Directive (NSDD) Number 145, "National Policy on Telecommunication and Information Systems Security" dated September 17, 1984; Office of Management and Budget Circular No. A-130 "Management of Federal Information Resources" dated December 12, 1985; General Services Administration, Federal Information Resources Management Regulation; and National Bureau of Standards, Federal Information Processing Standards Publication.

2. DISTRIBUTION. This order is distributed to the division level in Washington, regions, centers, and overseas area offices with a limited distribution to all field offices and facilities.

3. CANCELLATION. Order 1600.54A, Security of FAA Automatic Data Processing Systems and Facilities, dated March 20, 1984, is canceled.

4. BACKGROUND. Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the Government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems, as well as those which process the private or proprietary information of U.S. persons and businesses, can become targets for foreign exploitation.

a. Within the Government, these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States.

b. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the Government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities.

c. Paragraphs 4a and 4b are quoted from NSDD-145, and, as stated in the past, computer systems play an essential role in accomplishing the operational, administrative, and managerial tasks performed within FAA. Consequently, computer equipment, the facilities housing or supporting AIS-related activities, and the data processed by FAA computer systems represent important organizational assets which must receive protection commensurate with their importance and value. This worth is measured in terms of aviation safety, capital investment, and organizational dependence upon FAA computer systems.

d. A highly sophisticated system of telecommunications and special purpose computers has been created to exercise positive air traffic control and facilitate the efficient movement of civilian and military aircraft within the airspace of this country. The conversion from manual methods of ATC to a semiautomated system has resulted in a significantly changed operational environment at FAA ATC facilities and support installations. These operational changes have also had a corresponding impact upon the security program at each of the facilities housing special purpose computer equipment used either in actual ATC operations or to support these functions by performing training, program development, or communications processing missions. As this system is modernized in the coming years, more and more reliance will be placed on automated processes, each have a need for better means of security protection.

e. The extensive use of data processing to accomplish record keeping and other administrative functions, together with the rapidly evolving technical sophistication of computer systems, has created a new information handling environment of great potential risk. Computer hardware and software developments have enhanced the ability to create large concentrations of data in host computers, which may be accessed quickly by users either locally, or remotely over a communications network. These factors require the creation of data access controls which afford protection at least equal to, and hopefully superior to, the controls now used in manual filing systems to safeguard vital organizational data, national security material, and sensitive personal information. The benefits to be derived from the many and varied uses of computer systems are substantial. These advantages, however, must be accompanied by new techniques to safegaurd data and resources from misuse or abuse. Protection is needed for proper accessing by authorized users, unauthorized disclosure or transfer of data, disclosure of security mechanisms, manipulation or deletion of this information.

f. The Federal Government, in the past, has suffered some catastrophic losses to various computer installations, to include loss of human life, irreplaceable data and equipment, and denial of essential data processing support. The Comptroller General has concluded recently that computer security practices in the Federal Government have not provided the necessary insurance that data processing assets are properly protected. This order seeks to recognize the importance of computers to FAA operations and establishes a cost-effective security program to safeguard these hardware, software, data, personnel, and facility resources.

g. There is a large set of factors which can contribute to the protection of the Data Processing Activity (DPA) and the data stored or processed within its physical confines. It is universally recognized that no Data Processing Installation (DPI) or computer system can ever be made completely secure against crime, physical damage, unauthorized access to data, or interruption of services. It is possible to determine what particular combination of security measures will provide a reasonable level of security at an acceptable cost through the use of risk management techniques. Risk management applied to the security of data processing operations utilizes quantitative methods together with the informed judgments of responsible managers to identify and optimize appropriate security controls.

h. Computer security risk management is concerned with identifying, controlling, and minimizing the impact of adverse events upon the data processing facility and FAA organizations that depend upon automated processes and operations. The object of the risk management process is to:

(1) Provide decision makers with sufficient information to determine the level of the risk present at FAA DPI's.

(2) Optimize the available agency resources that can be allocated to implement and to maintain the physical, administrative, and technical security controls required to assure an adequate level of security for an AIS system.

i. Risk analysis is the systematic study and analysis of a particular DPA. A thorough risk analysis constitutes the first step for the development of an effective computer security program. In recognition of this fact, the use of risk analysis techniques has been mandated by the Governmentwide policy directives cited in Appendix 2.

5. EXPLANATION OF CHANGES. This revision:

a. Contains new requirements mandated by National Security Decision Directives (NSDD) Number 145, National Policy on Telecommunication and Automated Information Systems Security.

b. Contains the requirements of Office of Management and Budget Circular No. A-130, Management of Federal Information Resources.

c. Contains the requirements of Public Law 100-235, The Computer Security Act of 1987.

d. Contains the requirements of General Services Administration, Federal Information Resources Management Regulation.

e. Contains a new chapter on Computer Processing of Classified Information.

f. Contains a new chapter on Office Automation Systems.

g. Expands Chapter 10, Contingency Planning, to include a core contingency plan for the air route traffic control centers.

h. Rewrites Chapter 11, Risk Analysis of All Computer Facilities, as the present method of risk analysis has been deleted and replaced with Los Alamos Vulnerability Assessment (LAVA) and a short form risk analysis.

i. Contains a new Chapter 13, Training and Automated Information Systems Security Awareness.

j. Contains a new Chapter 14, Specific Requirements for Connectivity and FAA Overseas Systems.

k. Contains a new Chapter 15, Accreditation.

l. Updates the appendix on the updated glossary of terms.

m. Contains Appendix 3, Short Form Risk Assessment.

n. Contains Appendix 4, Contingency Plan for ARTCC.

o. Includes a new Appendix 5, Subject Index, to make it easier to research this order.

p. Deletes several appendices from the previous order.

6. DEFINITIONS AND SUBJECT INDEX. Definitions for the terms used in this order are contained in Appendix 1, Definition of Terms. Appendix 5, Subject Index, contains an index to assist users of this order and to make it a workable reference document.

7. FORMS AND REPORTS.

a. FAA Form 1600-57 (2-88), RIS: CS 1600-28, Short Form Risk Assessment is described in paragraph 703f and 1105b. This form may also be used as a DPA Security Profile. A copy of this form shall be completed for each Office Automation (OA) system and submiited as accreditation documentation described in paragraph 1503. Local reproduction of this form is authorized.

b. FAA Form 1600-56 (2-88), RIS: CS 1600-29, Letter of Agreement is described in paragraph 911. Permission must be approved, and copies of the request and agreement maintained by the identified personnel. Local reproduction of this form is authorized.

c. RIS: CS 1600-30 LAVA/CS Vulnerability Report, this report is described in paragraph 1105b. Copies of these reports shall be maintained at the FAA facility with a copy fowarded as accreditation documentation described in paragraph 1503.

d. RIS: CS 1600-31 Contingency Plan, is described in Chapter 10, with guidelines for development in Appendix 4. This report shall be submitted with the accreditation documentation outlined in paragraph 1503.

e. RIS: CS 1600-32 Request for Accreditation, this report shall be submitted in the form of a memorandum with the required attachments, outlined in paragraph 1503.

f. RIS: CS 1600-33 Statement of Accreditation, this report is described in paragraph 1504. The report shall be in memorandum format and a copy shall be maintainned for each AIS.

8. STATEMENT OF POLICY. It is FAA policy to provide an adequate level of security for FAA general and special purpose computer equipment, telecommunications systems, the installations housing or supporting the operation of such computer and telecommunications equipment, and the data processed or transmitted by these systems. Security measures utilized to obtain this objective will be cost-effective and reflect the relative importance of each computer facility to FAA missions, the sensitivity or criticality of the information processed, and the monetary value of computer-related assets. This policy is to be implemented by:

a. Designating an official to be responsible for coordinating the FAA AIS Security Program.

b. Establishing minimum FAA security standards applicable to FAA computer systems and facilities.

c. Assuring that risk management techniques are applied in determining the most cost-effective security measures required for any FAA computer facility.

d. Assuring that security certifications of sensitive systems or applications are accomplished in a timely fashion.

e. Assuring that the accreditation of all appropriate systems or applications are accomplished in a timely fashion.

f. Assuring periodic inspections of major FAA DPI's are accomplished to measure and evaluate compliance with established national standards and/or local security controls implemented as a result of a risk analysis.

g. Maintaining effective liaison with other Government and private groups active in the field of AIS security, particularly the National Bureau of Standards (NBS) and the National Computer Security Center (NCSC).

9. SCOPE.

a. This order applies to all offices, services, regions, and centers which use, operate, or control Automated Informations Systems, which include general and special purpose computer systems and telecommunications systems. It further applies to facilities that use contractor-provided data processing services such as commercial time-sharing. Variances in degree of applicability resulting from different operational uses of Automated Information Systems are addressed in the body of this order. Automated Information Systems are broken down into classes of computers as follows:

(1) Microcomputer

(2) Minicomputer

(3) Superminicomputer

(4) Large Mainframe Computer

(5) Plug-Compatible Mainframe (PCM) Computer

(6) Communications computer

b. FAA computer equipment located on military bases or in buildings owned and controlled by other Federal agencies or by state, local, or regional authorities is governed by the provisions of this order. Problems in complying with this order which result from either conflicting policies or constraints imposed by the cognizant authority owning or controlling the property will be referred to the appropriate supporting security element for resolution.

c. AIS security standards established (see Order 1350.22A, Protecting Privacy of Information About Individuals) with regard to the processing of personal information covered by the Privacy Act of 1974 apply to general purpose and to special purpose computer systems when these systems are used to process data covered by the Privacy Act.

d. Programmable electronic calculators and analog computers are excluded from the provisions of this order. Security standards for this type of equipment are set forth in Order 1600.6B, Protection of Agency Property.

e. Office automation systems inclusive of stand-alone data processing equipment, word processors, and systems with telecommunications capabilities are covered by the provisions of this order. The physical security of these machines and their use in processing classified information is contained in chapter 5.

f. Personnel security requirements for AIS are specified in paragraph 205b.

g. New software systems or computer equipment developed, designed, or procured after the effective date of this order are subject to the provisions of this order before any action is taken. All AIS shall be reviewed for accreditation in compliance with chapter 15. Existing installed equipment and/or existing hardware systems that do not meet the security provisions of this order may be granted a temporary accreditation. The purpose of the temporary accreditation is to allow time for the management of the system to make the necessary changes to the system to bring it into compliance with this order.

10. RESPONSIBILITIES.

a. The Administrator has authority and administrative control over all FAA personnel and property. The Administrator is also responsible for assuring that FAA general purpose and special purpose AIS activities are in compliance with appropriate statutes, executive orders, and other Federal regulations pertaining to the use and protection of AIS resources. The Administrator is the Designated Approving Authority (DAA) for all AIS and networks processing Level I data.

b. The Director of Civil Aviation Security, ACS-1, is responsible for:

(1) Developing, coordinating, and implementing a comprehensive FAA AIS Security Program for both general purpose and special purpose computer systems.

(2) Assuring that plans, policies, and procedures have been implemented by responsible operating components to establish and maintain appropriate administrative, physical, personnel, environmental, communications, and hardware/software security measures for FAA DPI and AIS.

(3) Developing plans and programs, recommending policies, and establishing procedures and techniques that will assure the creation of adequate physical security controls for facilities which house FAA computer equipment and supporting utilities.

(4) Assuring that the personnel security aspects of the AIS Security Program are accomplished in accordance with Order 1600.1C, Personnel Security Program.

(5) Serving as the focal point within FAA for coordinating the use of communication security (COMSEC) techniques or equipment in conjunction with the operations of Automated Informations Systems.

(6) Serving as the focal point within FAA for coordinating the use of AIS and communications equipment for the processing of classified information with the National Security Agency.

(7) Developing specific guidance and policies to regulate the computer processing and transmission of classified national security information by FAA computer systems.

(8) Developing, in cooperation with the Director of Management Systems, AMS-1, comprehensive security standards to cover the computer processing of information covered by the Privacy Act of 1974.

(9) Representing FAA at meetings with other departmental components, interdepartmental groups, or specialized organizations on all matters relating to AIS security and telecommunications security.

(10) Initiating, coordinating, and conducting, in association with other affected components, system security studies of FAA computer systems and evaluations of regional and center implementation of the AIS security program.

(11) Developing and implementing a comprehensive FAA AIS Security Risk Management Program.

(12) Serving as the National AIS Security Risk Management Officer for FAA.

(13) Assuring that security certification of sensitive systems or applications are accomplished.

(14) Serving as the focal point within FAA for coordinating the use of AIS for the processing of classified information with the National Security Agency.

(15) Designating a National AIS Security Program Manager.

(16) Assuring that the accreditation of all appropriate AIS are accomplished as required.

(17) Responsible for reviewing the accreditation documentation and making recommendations to the Administrator for AIS and communication networks that handle or process Level I data.

(18) Serves as DAA for stand alone OA systems processing Level I data at Washington headquarters.

(19) Serves as the DAA for Washington headquarters and National FAA AIS that process Level II data.

c. The National AIS Security Program Manager (AISSPM), is responsible for:

(1) Serving as the action officer for the AIS Security Program.

(2) Developing and recommending a FAA AIS risk analysis methodology applicable to AIS and telecommunications networks.

(3) Exercising program management responsibilities for the FAA AIS Security Program.

(4) Monitoring development of new AIS security risk management techniques and methodologies.

(5) Conducting evaluations of the effectiveness of the FAA AIS Security Program.

(6) Requiring additional risk analyses to be performed when a condition, event, or development may exist that exposes FAA or the public to an excessive level of risk. Making recommendations to the Director of Civil Aviation Security for waiver of a requirement to perform a risk analysis under conditions of significant change (as defined in appendix 1) based on a justified appeal in writing from the responsible FAA component.

(7) The AISSPM is responsible for chairing a steering committee to assure that a risk analysis is conducted on the total NAS utilizing a total system approach to determine where vulnerabilities now exist and which subsystem(s) are the most cost-effective security safeguards that should be implemented. Further the AISSPM will assure necessary updates are performed in accordance with paragraph 10c(6) or when a new system is added to the NAS.

d. The National AIS Security Program Manager Deputies (AISSPMD) are responsible for:

(1) Serving as the deputy action officer for the AIS Security Program.

(2) Assisting the AISSPM in exercising program management responsibilities for the FAA AIS Security Program.

(3) Serving as AIS security advocate for assigned regions and centers.

e. Headquarters AIS Security Program Manager, is responsible for:

(1) Serving as the AIS Security action officer for Washington headquarters.

(2) Reviewing specifications and procurement documentation to ensure needed AIS security requirements are included for nationally developed systems.

(3) Reviewing accreditation documentation and making recommendations to ACS-1, when ACS-1 is designated approving authority.

f. Directors of offices and services, are responsible for:

(1) Assuring that the security responsibilities inherent in the management function for FAA general purpose and special purpose computers are met through the development and implementation of appropriate administrative, physical, technical and procedural security controls.

(2) Assuring that appropriate AIS security measures or techniques are considered and used in the development, design, acquisition, and testing of DPA.

(3) Submitting acquisition documentation to the Office of Civil Aviation Security as stated in paragraphs 205a, 205b, and 205f. Security must be addressed from a total systems approach.

(4) Submitting design, modernization, and construction specifications for DPA to the Office of Civil Aviation Security (ACS) for review and approval.

(5) Requesting approval from ACS to process classified information.

(6) Coordinating and planning, with ACS, for the operational use of COMSEC equipment in a DPA.

(7) Assuring that an Automated Information Systems Security Manager (AISSM) is appointed for DPI's under their operational control.

g. Regional Administrators and Center Directors will be the DAA for all AIS for which they have operational control and for AIS and communications networks which handle or process Level II data. He/she will also be the DAA for stand alone OA Systems which process Level I data.

h. Manager, Civil Aviation Security Division/Staff of regions, centers, and Europe, Africa and Middle East Office are responsible, in their respective jurisdictions, for:

(1) Exercising program management responsibilities for the FAA AIS Security Program.

(2) Ensuring that an Automated Information System Security Coordinator (AISSC) is appointed.

(3) Responsible for reviewing all accreditation documentation for applicable systems and making accreditation recommendations to the DAA. Responsible for forwarding the completed accreditation documentation to the DAA for final disposition.

i. The Regional/Center Automated Information Systems Security Coordinator (AISSC) will act as a focal point for all AIS security matters in his/her cognizant region/center. A position description will be established for each region/center AISSC to include AIS security responsibilities as the primary job function. The AISSC will be designated in writing to the AISSPM by the regional/center security division or staff manager. AIS security responsibilities, as described in this order, shall be established as a critical job element and the performance standards for these responsibilities shall be outlined in the employee's general performance appraisal document.

Major responsibilities include, but are not limited to, the following:

(1) Manage the development, implementation, and execution of the FAA AIS Security Program within the cognizant region/center.

(2) Ensures that a regional/center AIS Security Inspection Schedule and Plan is developed and maintained in accordance with FAA Order 1650.7B.

(3) Monitors National AIS System Inventory Directory (SID) system of all region/centers. Ensures all systems identified are accurately reflected in the region/center AIS Security Inspection Schedule and Plan.

(4) Maintains a status report of AIS accreditation documentation (i.e., risk analysis, action plans, standard operating procedures, contingency plans, etc.) which has been completed for each DPA within the cognizant region/center.

(5) Ensuring that an Automated Information System Security Manager (AISSM) is appointed for each Data Processing Installation (DPI).

(6) Establishing an AIS Security Training and Awareness program.

(7) Ensuring that all AIS security incidents or violations are investigated, documented, and reported.

(8) Ensuring that all procurement documents or specifications developed within the region/center comply with appropriate AIS security requirements.

(9) Reviewing all accreditation documentation and making recommendations to the Civil Aviation Security Manager and the DAA regarding accreditation.

j. The Automated Information Systems Security Manager (AISSM) will be appointed for each DPI. The AISSM responsibilities involve coordination of all AIS security matters with the cognizant AISSC. AIS security responsibilities as described in this order shall be established as a critical job element and the performance standards for these responsibilities shall be outlined in the employee's general performance appraisal document. In initiating new or revised position descriptions, these responsibilities must be included. Major responsibilities include, but are not limited to:

(1) Acting as focal point for all AIS security matters concerning the DPI to which appointed.

(2) Maintaining an inventory of all DPA's under his responsibilities.

(3) Reporting all changes in the inventory to the AISSC.

(4) Assigning an Automated Information Systems Security Officer (AISSO) for each DPA.

(5) Acting as the DAA for all AIS processing Level III data in accordance with chapter 15 and paragraph 14.

k. The Automated Information System Security Officer (AISSO) will be appointed for each Data Processing Activity (DPA). An individual may be assigned AISSO responsibilities for more than one AIS. The AISSO responsibilities involve planning, development, and implementing AIS security measures for assigned DPA. The AIS responsibilities shall be identified as a job element in the employee's general performance appraisal document. Major responsibilities include, but are not limited to, the following:

(1) Acting as focal point for all AIS security matters concerning the DPA to which appointed.

(2) Executing the AIS Security Program as it applies to the assigned DPA(s), including preparing and submitting AIS security documentation to the AISSM.

(3) Maintaining an inventory of all hardware, implemented software, and major functional application systems and reports all changes to the AISSM.

(4) Monitoring system activity, including identification of the levels and type of data processed by the system, and controls user access to the system by enforcing standard security operating procedures.

(5) Preparing, coordinating, and submitting the appropriate system accreditation documentation in accordance with Chapter 15 of this order.

l. The Network Security Officer (NSO) will be appointed for each network by the AISSC. The responsibilities of the NSO involve AIS security management and problem resolution relating to the communication resources of the DPI. If communications networks are used to exchange data between DPI's, a single NSO will be appointed by the AISSPM to manage AIS security for each network, at the national level. The NSO is responsible for:

(1) Preparing, coordinating, and submiting the appropriate system accreditation documentation for the network in accordance with chapter 15.

(2) Maintaining user access profiles, including network user ID, password, and other authentication/access control variables for the assigned network.

m. The Terminal Area Security Officer (TASO) will be appointed by the AISSO to enforce all AIS security requirements for the DPA. Major responsibilities include, but are not limited to:

(1) Establishing and maintaining a listing of all authorized terminal users for assigned area.

(2) Maintaining terminal user profiles, including user ID, password, and security clearance.

(3) Providing the AISSO with a copy of the listing and profiles of personnel designating them as authorized terminal users.

(4) Limiting access to remote terminals by unauthorized users and enforces security operating procedures.

11. AIS SECURITY REVIEW AND ANALYSIS TEAMS. FAA headquarters, regions, and centers shall establish AIS Security Review and Analysis Teams, which will serve as expert advisors for the implementation of this order. Members of the AIS Security Review and Analysis Teams shall participate in the required risk analysis and security certification of sensitive systems. Members of the national team may participate in all other teams. The teams will be structured as follows:

a. FAA Headquarters and National Team.

(1) The National AIS Security Program Manager shall serve as the chairperson of the FAA headquarters and national team.

(2) The AISSM from the Management Systems organization, will serve as the cochairperson of the team.

(3) The appointed AISSO's and NSO from the major national sensitive applications (such as CPMIS, UPS, UAS, etc.) will serve as members of the team.

b. FAA Regional Team.

(1) The regional AIS Security Coordinator (AISSC) shall serve as the chairperson of the respective regional team.

(2) The AISSM, from the Management Systems organization or representing the Management Systems function, shall serve as the cochairperson of the regional team.

(3) The appointed AISSO's and NSO from the major sensitive applications (such as CPMIS, UPS, UAS, etc.) will serve as members of the team. Also, the AISSM's and AISSO's shall serve as members of the team.

c. The FAA Aeronautical Center Team.

(1) The AIS Security Coordinator (AISSC) shall serve as the chairperson of the Aeronautical Center team.

(2) The Data Services Division (AAC-300) AISSM shall serve as the co-chairperson of the team.

(3) The appointed AISSO's and NSO from the major sensitive applications (such as CPMIS, UPS, UAS, etc.) shall serve as members of the team.

d. The FAA Technical Center.

(1) The AIS Security Coordinator (AISSC) shall serve as the chairperson of the Technical Center team.

(2) The Management Systems AISSM shall serve as the cochairperson of the team.

(3) The appointed AISSO's and NSO from the major sensitive applications (such as CPMIS, UPS, UAS, etc.) shall serve as members of the team.

12. CONTRACTOR SUPPORT. If portions of risk analyses and/or security certification of sensitive systems are performed by a contractor, then the National AIS Security Program Manager shall serve as the Contracting Officers Technical Representative (COTR).

13. AIS SECURITY PROGRAM ELEMENTS.

a. The traditional approach to protecting important operational, informational, and organizational assets has been to create a secure operating environment through the use of appropriate physical, personnel, technical, communication, and administrative controls. However, the growing sophistication and complexity of modern computer systems have diluted the effectiveness of these traditional security techniques. The details of implementing an effective AIS Security Program at any DPI will vary due to the existence of such variables as the size, location, configuration, and sophistication of the DPA, the mission the system performs, and the pre-existence of facility security safeguards. However, certain common program elements can be identified which provide a general methodology that can be used to address the problem of AIS security. These include:

(1) Physical protection of the AIS equipment, facilities, data files, and supporting utilities.

(2) Assuring the honesty, trustworthiness, and positive attitude of personnel who manage, operate, program, and use an FAA AIS or communications system.

(3) Implementation of operational and administrative procedures and controls.

(4) Protection of data communicated between DPA's and/or remote terminal locations.

(5) Hardware and software safeguards that function to identify and verify users, restrict user access, maintain the integrity and reliability of system operations, or assist in establishing accountability for transactions accomplished through the system.

b. Accordingly, it is the purpose of this order to address the security problems posed by the use of AIS within FAA in the multidisciplinary approach suggested above. Through the systematic use of applicable physical, personnel, communications, administrative, and AIS security techniques, the protection of AIS equipment and data can be maintained at a satisfactory level. Aside from the basic mandatory requirements imposed by this order, additional safeguards implemented at any FAA DPA should be based upon a risk analysis.

14. ACCREDITATION. A Statement of Accreditation will be required for all AIS within FAA in accordance with chapter 15 of this order.

15. PROCESSING LEVELS. Within FAA data processed or transmitted by any AIS or communications computer will be categorized into a specified processing level. Level I data is classified National Security Information. Level II data is Unclassified Sensitive Data to include Privacy Act Data. Level III data is unclassified nonsensitive data. If an AIS processes more than one level of data, the AIS shall be protected and accredited to the highest level of data processed on the system.

16. MODES OF OPERATION. The mode of operation is a statement of the security environment and method of operating an AIS or communications computer. The following are the descriptions of each of the modes of operation.

a. System high security. The mode of operation in which system hardware/software is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.

b. Dedicated security mode. The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. This sometimes may be referred to as periods processing.

c. Multilevel security mode. The mode of operation which allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.

17. ORDER CONTENT AND ORGANIZATION. Due to the fundamental differences in the uses of AIS and communications security services within FAA, attempts have been made, where necessary, to provide specific security guidance which reflects the different operational uses and geographical locations that characterize the diverse use of AIS within FAA.

18. PROGRAM AUTHORITY. The requirement to conduct risk analyses and certification of FAA data processing activities is established in the Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," dated December 12, 1985, appendix III, paragraph 3.C(2). This circular requires Federal agencies to conduct periodic risk analysis of each AIS installation (microcomputer to large scale computer systems) and to perform certification of sensitive applications.

19. INTERPRETATION. Questions on interpretation of the provisions of this order or their application shall be referred to the appropriate regional/center or headquarters security element, appropriate element of the responsible office or service, or to the National AIS Security Program Manager.

20. AUTHORITY TO CHANGE ORDER. Authority to issue changes to this directive is delegated to the Director of Civil Aviation Security, ACS-1, except changes in policy, authority, and responsibility.

21. RESOURCES. Resource requirements resulting from the implementation of the order shall be justified and requested in accordance with existing budgetary procedures. Individual offices, services, regions, and centers should program or request funds as necessary to provide adequate security for all DPA's under their control. Budgeting and funding for national systems will be performed at FAA headquarters level.

22.-199. RESERVED.

CHAPTER 2. AIS SECURITY PLANNING, TESTING, AND EVALUATION

200. GENERAL. The achievement and maintenance of an adequate level of security at any FAA Automated Information System (AIS) Data Processing Installation (DPI) or Data Processing Activity (DPA) require the interaction of two distinct but interrelated processes, security planning and effectiveness verification.

a. Security Planning. Effective planning is the basic prerequisite for implementing any cost-effective system of security controls. Beyond some basic safeguards which can be prescribed for each FAA DPA, no standardized or universal solutions will satisfy completely the security requirements of every DPA. The existence of such variables as size and location of facility, technical complexity of the computer system, and the sensitivity of data processed necessitate the use of risk analysis techniques in determining specific security measures suited to a given facility. The application of risk analysis to the security planning process will result in a better understanding of vulnerabilities and provide a sound basis for the selection of the technological, physical, and administrative safeguards that may be required to provide an adequate security environment. As virtually every security control that can be utilized has some incremental cost, the importance of sound security planning cannot be underestimated. The basic elements of risk analysis are discussed in paragraph 203.

b. Effectiveness Verification. A continuing process of inspection, testing, analysis, and evaluation is required to assure that the security measures applied to a given facility are sufficient to protect physical AIS resources against natural and human threats and to assure the data processed by a system are adequately safeguarded against unauthorized or accidental disclosure, modification, or destruction. The effectiveness verification program is the responsibility of the Office of Civil Aviation Security and is consistent with other security inspection programs conducted in accordance with FAA orders set forth in appendix 2. All inspections will be conducted in accordance with Order 1650.7B.

201. SCOPE. The provisions of this chapter are intended to apply to all FAA AIS (general purpose and special purpose computer systems). It is recognized that the level of security planning required will vary in proportion to such factors as system complexity, facility construction, and the existing security environment.

202. PRIVACY ACT REQUIREMENTS. The Privacy Act of 1974 imposes numerous requirements upon Federal agencies to prevent the misuse or compromise of data concerning individuals. DPA's which process Privacy Act data are, therefore, required to provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of data, whether intentionally caused or resulting from accident or carelessness. The guidelines furnished in this order,

FIPS PUB #41 and FAA Order 1350.22A, Protecting Privacy of Information about Individuals, provide AIS installations with the appropriate FAA administrative, technical, and physical safeguards to implement the security requirements of the act. It is recognized that each AIS installation has a unique set of requirements and risks to consider depending on the installation's personal data processing mission and its operating environment. The requirement to protect information subject to the act shall be given appropriate consideration in the security planning process.

203. RISK ANALYSIS. The achievement of an adequate, cost-effective level of security for any FAA automated information system (computer) facility necessarily involves the selection from among various alternatives. Given the variances in facility configuration, and differences in system sophistication and relative importance, the particular set of security measures needed at any AIS facility must be determined by analyzing a complex set of conditions. The use of the Los Alamos Vulnerability Assessment (LAVA) represents an overview of what is needed to provide a realistic analysis of security hazards. Once significant threats are identified, cost-effective security options can be presented to management for consideration. Management must decide as to what risks can be tolerated and those which must be controlled by the allocation of resources. Chapter 11 and appendix 3 set forth the procedures for risk analysis for all computer facilities. An extensive risk analysis is not required or suggested for all FAA computer systems; however, the use of this technique is particularly applicable to the larger and more complex facilities housing sophisticated computer assets.

204. BASIC AND SUPPLEMENTAL CONTROLS. The completion of the risk analysis and planning process will result in the identification of two fundamental types of security controls. These are:

a. Basic Security Controls. Of primary importance in creating an Automated Information System (AIS) Security Program is the establishment of a base level of security. This order will identify the major components of this base by requiring that certain physical, environmental, and procedural measures be implemented. The purpose of these security controls is to establish fundamental security of AIS operations within FAA. Unless this security base is established and maintained, the effectiveness of any supplemental security measures will be negated.

b. Supplemental Security Measures. Depending upon the sensitivity of the data processed by a system, the dependence of the organization upon the system, and the nature of the security threats to a particular data processing activity, additional security controls may be required. Hardware/software, operational data, and, where applicable, COMSEC measures represent the primary types of locally implemented security measures which can be used to enhance or supplement mandatory security standards. The selection of these controls should be based upon data developed during the risk analysis process which indicated which combination of additional security measures are needed to further reduce the level of risk.

205. AIS SECURITY EFFECTIVENESS VERIFICATION PROCEDURES. Several different techniques will be utilized to verify that an adequate level of security is considered in the acquisition of new AIS equipment and software or is present at each DPA, at each remote access point, and in each computer system. These include:

a. Review of National FAA Acquisition Documentation for AIS. In accordance with Order 1370.52B, Information Resources Management Policies and Procedures, the Office of Civil Aviation Security shall review the documentation for the acquisition of National AIS and communications equipment, software, and services from the computer security standpoint to insure compliance with the security requirements set forth in this order and OMB Circular A-130.

b. Personnel Security.

(1) All individuals, contractor and Government, participating in the design, development, operation, or maintenance of AIS Level II applications, as well as those having access to Level II sensitive data shall be screened in accordance with Order 1600.1C, Personnel Security Program.

(2) All contractor personnel participating in contracts involving Level I information shall be screened in accordance with FAA Order 1600.56, Guidelines for FAA Participation in the DOD Industrial Security Program (ISP).

(3) All Government personnel involved with Level I information shall be adjudicated in accordance with Order 1600.1C.

c. Preliminary Security Site Surveys. In accordance with Order 1600.46, Physical Security Review of New Facilities, Office Space or Operating Areas, prior to the construction or major modification to a central computer equipment room, associated supporting facilities, or remote terminal cluster rooms, a preliminary security survey of the installation shall be conducted by the appropriate supporting security element. This may consist of a review of construction plans or an inspection of a room or facility to be used as a computer equipment area. The results of the survey will be utilized as a means for assuring that an appropriate base level of security is present before operational use is initiated.

d. Security Inspections. FAA general and special purpose computer facilities will be inspected for AIS security by the appropriate region or center security element in accordance with Order 1650.7B, Civil Aviation Security Program Guidelines. Locations housing remote terminals used to access FAA computer systems which process sensitive information, as defined by Order 1370.47A, Control and Handling of Sensitive Data in Automatic Data Processing Organizations, will also be included in this inspection program.

e. Periodic Risk Analysis. A risk analysis shall be performed:

(1) Prior to the approval of design specifications for new installations.

(2) Whenever a significant change occurs to the installations (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability). Agency criteria for defining significant change shall be commensurate with the sensitivity of the data processed by the installation.

(3) At periodic intervals established by the agency commensurate with the sensitivity of the data processed but not to exceed every 5 years if no risk analysis has been performed during that period.

f. Design Reviews and System Tests. The office of principal interest (OPI) shall conduct and approve design reviews and system tests, prior to placing the application into operation, to assure the proposed design meets the approved security specifications. The objective of the system tests shall be to verify that required administrative, technical, and physical safeguards are operationally adequate. The results of the design reviews and system tests shall be fully documented and maintained in the official agency records and submitted to the Office of Civil Aviation Security for final approval.

g. Comprehensive AIS Security Evaluations. The Director of Civil Aviation Security, with the prior coordination of appropriate managerial officials, is authorized to conduct comprehensive AIS security evaluations which address all facets of the AIS Security Program at an individual FAA computer facility. These will be conducted by specialists having appropriate technical skills who may be temporarily assigned to perform these evaluations. Contractor personnel may be utilized in the performance of these studies.

h. Certification of Sensitive Systems or Applications. After a risk analysis has been performed on a DPA, then certification of all local sensitive systems or applications at that facility will be performed. Details for certification are contained in chapter 12. If sensitive systems are involved, then a risk analysis must be performed on all DPA's involved before certification can be accomplished.

206. SPECIALIZED SECURITY STUDIES AND EVALUATIONS. The Director of Civil Aviation Security, with the coordination or at the request of the appropriate region, center, office, or service director, may conduct specialized AIS security studies on matters pertaining to the security and integrity of FAA computer systems. Once authorized, these studies may be performed by FAA or by FAA contractor personnel. Examples of the types of special studies that may be conducted under this authority include, but are not limited to:

a. System Integrity Study. A study of an interactive, general purpose software system to determine if a typical user may perform unauthorized accesses to data or system functions by exploiting weaknesses in software security controls and develop recommendations for correcting identified problems.

b. Fire Protection Study. Such an analysis will be accomplished to assure that key FAA computer facilities and personnel are adequately protected against the hazard of fire.

c. Developmental System Security Analysis. A study of this type would be accomplished to review requirements for and the adequacy of security measures designed intc major FAA computer systems under development.

207.-299. RESERVED.

CHAPTER 3. PHYSICAL SECURITY

SECTION 1. GENERAL PROVISIONS

300. GENERAL. This chapter establishes the requirement for minimum physical security standards based upon accepted basic AIS security practices identified in higher authority directives and those security standards required by Order 1600.6B.

a. Adequate, cost effective physical security is a prerequisite to achieving a secure data security environment. The ultimate goal of the FAA AIS security program is three-fold:

(1) To prevent unauthorized access or misuse of computer and computer related facilities.

(2) To detect an unauthorized access or misuse of computers and related facilities.

(3) To minimize losses and be able to recover from losses as efficiently as possible.

b. Total security for computer installations is unattainable. There is a definite need to provide a high degree of cost-effective asset protection for FAA AIS and facilities. The process of determining and justifying what physical protection measures are needed at any facility requires the use of an analytical risk analysis.

301. HAZARDS TO DATA PROCESSING INSTALLATIONS. In the development of a physical security system for any FAA AIS, security planners must consider the types of threats to which the installation and data processed or stored within the facility could be subjected. These include, but are not limited to:

a. Access to a central computer facility or remote terminal area by unauthorized individuals.

b. Acts by employees or other personnel to include deliberate theft, modification, or unauthorized disclosure of data.

c. Equipment interruptions or failures caused by destroying or damaging supporting utilities.

d. Occurrence of accidents or natural threats as fire, flood, wind, or earthquakes.

e. Improper use and control of secondary office equipment such as memory typewriters, copy machines, etc.

f. Improper or careless use of an DPA or remote terminal area by authorized individuals (this can include computer maintenance personnel, programmers, cleaning personnel, and others that work on computers on a daily basis).

g. Lack of awareness or concern for sensitive information and AIS security procedures.

h. Employee carelessness and errors.

i. Malfunction of equipment, resulting in denial of service to users.

j. Survielance or other electronic intercepts of signals generated by computers or other conveyances.

302. PHYSICAL SECURITY PRINCIPLES. The diversity of AIS and installations within FAA make it undesirable to establish universal, rigid physical security standards. However, it is also recognized that the establishment of an adequate physical security environment for each FAA AIS is necessary. This is achieved through the implementation of cost-effective physical security principles enumerated below:

a. Positive physical personnel access controls shall be established to prevent unauthorized entry into the computer room and other critical areas which support or affect the operation of computer equipment or the processing of data by this equipment.

b. Physical access to data files and media libraries shall be prevented and controlled to the extent economically feasible by the use of cost effective security measures and well-conceived and tested emergency and contingency plans.

303. COMPUTER UTILIZATION. This chapter reflects the basic differences in computer utilization within FAA. The different operating environments, as well as other considerations, require different approaches, to achieving the same objective, be taken with respect to these two basic types of computer systems (general purpose and special purpose).

a. General purpose and special purpose computers are further broken down into categories of computers as follows:

1. Microcomputer

2. Minicomputer

3. Superminicomputer

4. Large Mainframe Computer

5. Plug-Compatible Mainframe Computer (PCM)

b. The following are examples of some of the computers in FAA:

1. General purpose microcomputer. The Field Office Modernization Program, Burroughs B21, B22, and IBM PC compatibles.

2. General purpose minicomputer. Southern Region, Data General Nova 4/C150.

3. General purpose superminicomputer. Headquarters, regions/centers new administrative computer, Data General MV-8000 and MV-15000.

4. General purpose large mainframe computer. Aeronautical Center, IBM 3084 system.

5. Special purpose minicomputer. ARTS II, ARTS III.

6. Special purpose large mainframe computer. ARTCC, IBM 9020 and HOST computers.

304.-309. RESERVED.

SECTION 2. SECURITY STANDARDS FOR GENERAL PURPOSE COMPUTER FACILITIES

310. GENERAL. The following are standards and guidelines for establishing a physical security system at general purpose computer facilities. These guidelines are also relevant to the design and construction of special purpose computer facilities.

311. CENTRAL COMPUTER COMPLEX SITE SELECTION CRITERIA. Site selection is a key factor in the establishment and maintenance of a secure operating environment at a FAA DPA. Ideally, the physical characteristics of any location selected to house a general purpose computer system must support the establishment of a physical security system at the facility. Architectural design is an equally important aspect of the site selection and security relationship. Although it is not desirable to establish firm FAA-wide standards governing the locations where general purpose (minicomputer, superminicomputer, large mainframe, plug-compatible mainframes) facilities may be located, the following points should be considered in the site selection process:

a. Below ground level installations or other locations possibly subject to flooding shall be avoided.

b. Windows shall be avoided in computer equipment rooms because of their inherent vulnerability to forcible entry, the loss of usable floor space, and problems associated with solar heating.

c. A location within a building that is easily accessible to the general public shall be avoided so as to minimize the exposure resulting from public traffic.

d. It is recommended that the equipment room be located in the center of the building. This ensures additional protection provided by the building.

e. Physical provisions for restricting access shall be incorporated into the initial design.

f. The existence or absence of activities above, below, or immediately adjacent to projected DPA's that might pose a hazard shall be established.

g. The requirement to provide protection for other critical areas, such as media libraries, data preparation areas, and environmental support equipment, must also be considered in the site selection and facility design process.

h. Electronic equipment should be installed in areas located where danger from fire, smoke, and explosion is minimal. A thorough survey should be conducted prior to site selection to identify potential threats to the equipment.

i. Factors to be considered for the selection of a building are structural designs to resist the effects of hurricanes, earthquakes, tornadoes, high winds, etc.

j. Where smoke or corrosive vapors may be introduced, or where fire detection, isolation, extinguishment, and egress considerations may be aggravated, partially compromised, or complicated due to the size and nature of the building or accessibility to the electronic equipment area, equipment shall be protected by such normal and extra measures as required by providing overhead waterproofing, floor drains, pumps, alarms, emergency waterproof covers, etc.

k. If the computer area is located against an exterior building wall, adequate protection shall be provided against security intrusion, fire, storm, and explosion.

l. Any electronic device that produces, transmits or stores an electronic signal (i.e. AIS, electric typewriters, telephones, etc.) are vulnerable to having these signals intercepted by electronic means. Individual rooms can be sheilded to minimize the danger of this type of intercept, but it is important to ensure that heating/cooling ducts and electrical lines to these rooms are also shielded. Rooms can also be shielded to minimize audio or acoustic surveillance.

312. HOUSING STRUCTURE (BUILDING). The physical security of computer rooms depends to a large extent upon the adequacy of the construction of the structure in which it is housed.

a. Existing structures used to house a computer room shall be either fire resistive or of noncombustible construction. Where deviation is of paramount necessity, an existing structure of combustible construction may be used to house equipment, provided the structure is completely protected by an automatic sprinkler system complying with all requirement of NFPA Standard No. 13, Sprinkler Systems.

b. New structures built to house a computer room shall be of fire resistive or noncombustible construction. All structural members, including walls, columns, piers, beams, girders, trusses, floors, and roofs, shall be of materials which are noncombustible or limited combustible, such as steel, iron, aluminum, brick, concrete, glass, ceramic tile, slag, plaster, etc., as opposed to materials which are inherently combustible but have been treated to give them fire retardant qualities. Asbestos containing materials shall not be used. Materials used for interior finishes, insulation, vapor barriers, shielding, or acoustical treatment shall have a surface flame spread rating of 25 or less (See NFPA No. 255, Test of Surface Burning Characteristics of Building Materials) and shall possess a "smoke developed" or specific optical density (Dm) of 450 or less (flaming). (See NFPA No. 258, Standard Test Method for Measuring Smoke Generated by Solid Materials.)

c. When a computer is to be housed in structures containing other occupancies, the following factors shall be considered to assure that the computer is not susceptible to danger as a result of fires in the other occupancies:

(1) In single story structures, computer areas shall be separated from other occupancies by fire rated walls or partitions. (See paragraph 313 for fire resistance ratings of these separating walls and partitions) The structure's framing system shall be designed so that a fire external to the computer area cannot cause a structural failure which will cause damage or structural collapse within the computer area.

(2) In multistory structures, computer areas shall be separated from other occupancies by two hour fire rated walls, partitions, floors and ceiling construction. The structure's framing system shall be designed so that a fire external to the computer area cannot cause a structural failure which will cause damage or structural collapse within the computer area.

(3) The floor above the computer room shall be provided with protection to prevent passage of accidental spillage, wash water, or other leakage. In any case, where there is a large quantity of water or a high potential of water spillage or flow, including that which might result from fire fighting operations on a floor above an electronic equipment area, a complete waterproof membrane should be provided and maintained. Where any serious potential of water spillage exists on the floor within the computer area, the necessary curbs, sills, and floor drains shall be provided.

(4) Automatic sprinkler protection shall be provided for all high hazard occupancies and for any moderate hazard occupancy not separated from the computer area by fire resistive construction having at least a 2-hour fire resistive rating. (See figure 3-1, Fire Hazard Classification of Occupancies, and paragraphs 362-369.)

313. <u>COMPUTER ROOM PERIMETER CONSTRUCTION STANDARDS</u>.

a. The requirements in this paragraph apply to single and multistory structures. They are designed to provide a fire resistive separation between the computer area and adjoining areas. This includes those areas located above, below or adjacent, including contiguous or abutting structures, yard storage, and industrial operations. The prime purpose of the perimeter separation is to protect the computer from the damaging effects of a fire outside of the computer area.

b. Fire resistive separations shall be of a noncombustible material having a fire resistance classification not less than the maximum fire potential of occupancies in adjoining areas or other adjacent, contiguous, or abutting structures, yard storage, and industrial operation (See figure 3-1 to determine the maximum fire potential). In no case shall the fire resistance classification be less than 1 hour. Fire resistive separations shall extend from structural floor to the underside of the structural floor or roof above.

c. In existing structures of combustible construction, fire resistive separations shall have a fire resistive classification of 2 hours or greater and should preferably start at the foundation and extend continuously through all stories and through the roof to form a parapet.

d. Opening in fire resistive separations shall be protected by fire doors, fire windows, fire dampers, or glass block, subject to the following:

(1) Fire windows or fire resistant glass block meeting the requirement of paragraph h. below may only be used for openings which are subject to light fire exposure and which are protected by automatic sprinklers.

(2) Fire doors meeting the fire resistance ratings prescribed in paragraph g. below shall be used on any door openings in the separation.

(3) Fire doors that serve as exit doors must swing with the exit travel except for doors on individual small rooms, which may swing in. Rolling or sliding doorsthat are not approved as exit doors shall not be used as exits.

(4) Because of the potential of smoke and fire damage, all opening in the separation, except ducts, should be protected with normally closed doors, fixed fire windows, or glass block.

(5) Fire dampers having a fire resistance rating of at least 1-1/2 hours shall be used in ducts at the point(s) where the duct penetrates the perimeter wall(s).

e. Fire resistance ratings of fire doors, fire dampers, fire windows, and fire resisting glass block shall be as determined and reported by a nationally recognized testing agency in accordance with "Methods of Fire Tests of Door Assemblies," NFPA No. 252, UL 10 (b), or ASTM E152.

f. Installation (including size limitations and hardware) of fire doors, fire windows, and glass blocks shall be in accordance with the requirements of NFPA No. 80, Fire Doors and Windows.

g. Fire resistance classification of fire doors shall be in accordance with the following table:

Fire Resistance Classification of Perimeter Separation	Minimum Fire Resistance Classification of Fire Doors for Openings
More than 2 hours -650 F Max (342 C)	3 Hour (A)* with Temp Rise
2 Hours	1-1/2 Hour (B)* with Temp Rise-30 min. - 650 F Max. (342 C)
Less than 2 Hours	1-1/2 Hour (B)* or (D)* or 1 Hour (B) with Temp Rise 30 Min.-650 F Max (342 C)

1 Hour	3/4 Hour (C)* or (E)*

* Denotes Fire Door Classification

NFPA #80 for explanation

h. Viewing windows and special architectural treatment for entrance doors may be provided in the separation, provided they do not violate the fire integrity of the separation. Some methods of accomplishing this are:

(1) The use of double sets of doors, one set of normally closed architecturally desirable doors of any construction, and a second set of fire doors held in the open position and released by the automatic fire detection system.

(2) When the fire exposure in the adjacent portions of the building is light and automatic sprinkler protected, a fire window assembly may be used for a viewing window.

(3) When extending the electronic equipment area to include a low fire hazard corridor, conference rooms, or similar area and installing the viewing window between this room or corridor and the electronic equipment, the requirements for fire resistive cutoffs and fire doors or other protected fire openings will then apply to the entire area included in the electronic equipment area.

(4) Limiting the viewing windows to the size of the fire doors and providing automatic fire door protection for such viewing windows.

i. The total area of all openings in a fire resistive separation, e.g., doors, windows, ducts, cable openings, sleeves, shall be as small as practicable and shall not exceed 25 percent of the total surface area from finish floor to finish ceiling of that separation in any plan or elevation.

j. Adequate fire stopping shall be provided to close penetrations of fire walls, fire partitions and floor slabs above and below the electronic equipment or similar purposes shall be sealed with material adequate to resist passage of heat, flame, and smoke for a period of time equal to the fire resistance rating of the building element penetrated. Concrete, grout, plaster or rockwool having adequate thickness, density, reinforcement, and anchorage may be used. A material or assembly specifically approved or listed for fire stopping by a nationally recognized fire testing laboratory may be used if, in addition, it provides adequate smoke control. Materials such as glass fiber and aluminum are not suitable because of low melting temperature.

k. Periodic inspections are essential to assure that the fire and smoke integrity of the electronic equipment area has not been violated by maintenance, operating, or installation personnel.

314. INTERIOR CONSTRUCTION OF COMPUTER AREAS. The requirements in this paragraph are designed to produce a computer area that will not itself provide the fuel for a disastrous fire.

a. When areas in an existing structure are to be converted for use as computer areas, all nonstructural combustible materials within the perimeter separation of the equipment areas shall be removed, except as permitted below:

(1) All materials installed within the perimeter separation of the computer areas including those used for walls, partitions, raised floors and their supporting systems, insulation, sound deadening boards, vapor barriers, acoustical treatments, furring strips, battens, duct work, and other constructions shall be noncombustible or limited combustible, except that minimum amounts of exposed combustible moldings and trim are permitted.

(2) When a raised floor system is to be installed in an area having a combustible finish flooring or floor covering, noncombustible materials shall be installed over the flooring or floor covering.

b. When raised floor systems are used in computer areas, they shall be of noncombustible materials, except that minimum amounts of vinyl or rubber materials are permitted for leveling, sealing, etc., or to prevent horizontal shifting of floor panels or decking.

(1) The structural supporting members for raised floors shall be noncombustible materials.

(2) Flooring, decking, and ramps shall be of non-combustible materials.

(3) Flooring or decking shall consist of easily removable access panels or sections provided in sufficient quantities so that power and signal cables, wiring, all space beneath the raised flooring or decking is accessible in case of emergency.

(4) Joints around floor panels or sections and openings in the flooring or decking for cables, wiring, or other uses shall be protected to minimize the entrance of debris or other combustibles beneath the flooring or decking. This may be accomplished by noncombustible covers, grilles, screens, gaskets, or by locating equipment directly over the opening joints. Cable and wire openings shall be made smooth or shall be otherwise protected to preclude the possibility of damage to the cables or wiring.

(5) Fascia or closure plates, which form side walls for ramps or edges of the flooring system, and handrails shall be of noncombustible materials.

(6) Commonly used floor covering materials, such as resilient floor tile and high pressure laminates, may be used on the raised floor deck. Carpeting is permitted if it is demonstrated that it is not readily ignited, does not build up a static level exceeding 3.5Kv when tested by the American Association of Textile Chemists and Colorists (AATCC) Test Method 134, and does not restrict lifting of panels for access to the under floor space.

c. If the structural floor in the electronic equipment area is lower than the adjacent structural floor, it should be equipped with an adequate drainage system. Provide backwater valves if there is any danger of water backing up through the system.

d. When the concealed space formed by a ceiling and floor assembly or ceiling and roof assembly is used as a supply or return air plenum chamber, the ceiling and plenum chamber installation shall conform with the appropriate provisions in NFPS No. 90A, "Air Conditioning and Ventilating Systems."

e. Ceilings shall be provided with access doors, panels, hatches, or other means of ready access to all portions of the concealed space above. In fire resistive ceilings, access panels shall be of construction equivalent in fire resistance to the ceiling ratings.

f. Fire resistant separations between separate electronic systems shall be of noncombustible or limited combustible materials having a fire resistance classification greater than the maximum fire resistance of less than 1 hour. Any openings in the fire resistant separations between the systems shall have equivalent fire rated protection. This fire resistant separation shall extend from the ceiling slab to the floor slab to include any concealed spaces above the ceiling and below the floor. When two or more adjacent systems are protected by automatic sprinklers in accordance with paragraph 363, the separation may be of any noncombustible materials with or without fire resistance rating.

315. ADDITIONAL COMPUTER ROOM STANDARDS. Other factors which will influence the design and construction of the computer room are identified in section 4 of this chapter.

316. COMPUTER ROOM ACCESS CONTROLS. Access controls are required to prevent unauthorized entry into the main equipment complex and to control the flow of materials into and out of the facility. Positive access controls will be maintained at all times to computer equipment rooms which house FAA general purpose computer systems. This shall be accomplished through the following means:

a. Designation as a Restricted Area. Each central computer room shall be designated and posted as a RESTRICTED AREA.

b. Control of Personnel Access During Operational Hours. Appropriate positive security controls shall be implemented to assure that only authorized persons are permitted to enter the computer room. This shall be achieved by maintaining a personnel access list and the use of one or a combination of the following: physical barriers, such as counters, locked doors equipped with electrical/electronic release, mechanical cipher locks, closed circuit television, receptionist, badge system, etc. It is highly desirable that a buffer or control zone be created immediately outside of the primary entrance to the equipment room. Use of secondary or emergency entrances will be strictly controlled and monitored.

c. Security of the Computer Rooms During Non operational Hours. All computer rooms housing general purpose computer systems shall be secured upon the completion of the business day or at any other time the facility is unoccupied, such as during a fire drill, bomb threat, etc. Strict accountability shall be maintained over keys and/or cypher lock combinations which permit access to the facility. A comprehensive security survey conducted by the supporting region or center security element may also disclose vulnerabilities in the afterhours environment. These may include entry into the computer room through the overhead crawlspace, beneath raised flooring, extending beyond the controlled area of the computer room, or though air conditioning vents or ducts.

d. Visitor Control. Positive controls shall be implemented at each FAA general purpose computer facility so that only authorized personnel are afforded unrestricted access to the equipment room. Appropriate visitor screening procedures shall be instituted to assure that other personnel permitted to enter the facility do so only after their identity and requirement for access have been verified by proper authority. Visitors shall be escorted by personnel identified on the access list.

317. PROTECTION OF CTHER ESSENTIAL OR CRITICAL AREAS. Within a general purpose computer complex, other work areas or support utility closets require physical security protection because of their importance to computer room operations, because they represent or contain valuable assets, or because unrestricted access significantly increases the threat to the confidentiality, integrity, and security of data files and applications software. The following areas shall be included in any risk analysis:

a. Data storage library

b. Remote input/output areas

c. Data conversion area

d. Programmers' area and files

e. Documentation files

f. Communications equipment area

g. Computer maintenance area

h. Utility room or closets

i. Telephone closets

j. Supplies storage

Physical security standards for some of the more critical areas identified above are specified in paragraphs 318 through 325.

318. SECURITY OF DATA STORAGE LIBRARIES. Areas used as storage locations for magnetic tapes, disc packs, paper tapes, or card decks associated with the operation of a general purpose computer system shall be afforded the following physical security protection:

a. A separate room for a record library shall be provided for functions requiring the use, manipulation, and storage of significant quantities or record materials.

b. The perimeter construction of the record library shall meet all the requirements of paragraph 313 and all subparagraphs except that the fire resistance rating of the separations shall be 2 hours or greater.

c. The perimeter construction of the computer area and the record library may include a common separation. The requirements for that portion of the separation which is common are:

(1) The separation has a 2-hour or greater fire resistance rating.

(2) If there are openings (a door or passthrough) between the record library and the equipment area, they shall be equipped with fire resistive closures having a 1-1/2 hour or greater rating.

d. The interior construction of the record library shall meet the requirements of paragraph 314 and all subparagraphs.

e. If the library is within the protected area of the central computer facility, it shall be provided with a solid door equipped with the FAA locking system. If the media storage area is located outside of the main computer facility, it shall be constructed in accordance with paragraphs 313 and 314 and the door will be provided with the FAA locking system. For those FAA general purpose computer facilities which do not presently have a separate media library room or area, appropriate measures will be taken to prevent the duplication, alteration, or theft of data and software. Additional security considerations for media storage areas include:

(1) Access Controls. Personnel access to media storage areas or containers shall be positively controlled by appropriate physical and procedural measure during operational hours. Highly sensitive data shall be further protected by locked storage cabinets. A limited personnel access list shall be posted inside the media storage areas or containers. One person will be designated as the media librarian and be accountable for contents of the library.

(2) Afterhour Protection. During periods when the computer facility is not operational or when reduced staffing does not permit effective supervision to be maintained, the door to library areas or cabinets which contain sensitive or proprietary fields or programs shall be secured. Depending on the sensitivity of the data, suitable alarm sensors may be provided.

(3) Environmental Protection. The unique fire and magnetic field protection requirements for data libraries are included in section 4 of this chapter.

319. SECURITY OF REMOTE TERMINALS USED TO ACCESS FAA GENERAL PURPOSE COMPUTER SYSTEMS. AIS operations usually require use of remote terminals. Remote terminals are subject to the same potential for abuse, damage, theft, and unauthorized use as those terminals that are located in a central computer facility, and generally the principles for assuring that adequate security is provided for the central computer facility terminals should be observed for those located at a remote site. Frequently, however, a remote terminal must be located in an area where those basic principles cannot be applied easily, and assuring adequate security may be more difficult and may require different and innovative procedures.

As noted later in paragraph 405, FAA remotely accessed general purpose computer systems are required to have the capability of disabling or disconnecting, either physically or by software, any or all of the remote terminals attached to the system. However, to assure adequate security at the remote terminal site, the following procedures shall be applied:

a. Physical Control

(1) Secured Area Concept. Where it is possible, a remote terminal shall be located in a room or area which is locked when the terminal is not under the immediate surveillance of an authorized user; i.e., use the procedures set out in sections 1 and 2 above for central facility terminals.

(2) Unsecured or Partially Secured Area Concept. If a lockable room is not available, the terminal shall be equipped with a disabling device and the terminal shall be disabled when the terminal is not under the immediate surveillance of an authorized user. This requirement is in addition to the disabling capability at the central computer facility discussed above concerning paragraph 405. A terminal can be disabled by a variety of methods, such as power disconnect locks or keyboard locks, with properly controlled key systems. In addition, consideration should be given to protecting the terminal from theft by installing a device that secures it to its work station. (i.e. lock-down or cable locking device). In determining the necessity to fasten the remote terminal to its work station, the attractiveness of the terminal in the market place, opportunity for theft, value of the terminal, and the cost of installing the securing device should be considered.

b. Administrative Control. Positive administrative safeguards shall be effected to assure that only authorized individuals are permitted to utilize those remote terminal equipment capable of accessing FAA computer systems. Appropriate caution shall be exercised to assure that sensitive information displayed on the screen is not viewed by unauthorized personnel, and that hard-copy output containing sensitive information is received and removed from the terminal area only by authorized individuals.

320. PROTECTION OF OFFICE AUTOMATION (OA) SYSTEMS. Microcomputers, personal computers, portable computers, and word processors shall be categorized as OA Systems. These OA Systems have the capability of accessing not only the FAA general purpose computers but other compatible computers. OA Systems are particularly subject to abuse, damage, theft, and unauthorized use. The guidelines provided in Chapter 9 shall be followed in order to provide adequate protection for OA Systems.

321. PROTECTION OF OTHER REMOTE ACCESS OR DATA ENTRY EQUIPMENT. Physical security safeguards for other remote access devices, example: Harris 1600 RJE Equipment, and the areas which house them, will be determined on a case-by-case basis by the using component and cognizant supporting security element. In general, the guidelines provided in paragraph 319 above shall be followed.

322. PROTECTION OF COMMERCIAL TIME-SHARING TERMINALS. Remote terminal devices used to access commercial time-sharing services shall be protected in accordance with paragraph 319 above.

323. PROTECTION OF WORD PROCESSOR WITH TELECOMMUNICATION CAPABILITY. All word processing equipment with tele-communicating capability to access general purpose and/or commercial time-sharing computers shall be protected as a remote terminal in accordance with paragraph 319.

324. PROTECTION OF PORTABLE TERMINALS. Because of their portability and opportunity for use in uncontrolled areas, management officials must take special care to assure proper use and protection of portable terminals. This equipment shall be used only in an area or in such a manner that sensitive data will not be exposed to unauthorized individuals. This equipment shall be stored in controlled space secured with a proprietary locking system when not in use. Removal of this equipment from a building is subject to property removal controls. In addition, a checkout log shall be maintained for this equipment which shows to whom the equipment is checked out, purpose for which its outside use is authorized, date and time of removal, and date and time of return. Users under these conditions shall assure that sensitive data and authenticators are not compromised by such use.

325. PROTECTION OF AIS ADMINISTRATIVE AREAS. AIS administrative areas are those areas associated with but do not house AIS equipment. The physical security considerations for such areas will vary considerably and the protective measure used will depend upon the determination made by the AIS management officials concerned in light of the sensitivity of the data involved. Consideration shall be given to:

a. Extent to which access to the area needs to be controlled while the materials are being handled.

b. Measure needed to protect the data concerned while the area is unattended, and

c. Measures needed to compartmentalize the AIS-related administrative function.

326. - 329. RESERVED.

SECTION 3. SECURITY STANDARDS FOR SPECIAL PURPOSE CENTER COMPUTER FACILITIES.

330. GENERAL. The successful completion of the initial phases of the National Airspace System (NAS) en route and terminal automation projects has resulted in increased FAA dependence upon the reliability and availability of computer support to effectively control air traffic and assure efficient utilization of the national airspace. In recognition of this importance, the following paragraphs prescribe the physical protective measure applicable to FAA computer facilities presently engaged in the actual control of air traffic or which are used to support this mission. The standards enumerated correspond to the general principles set forth in paragraph 302, but the unique operational requirements and environment of ATC facilities have been considered in establishing physical security standards. In the design and construction of new ATC computer facilities, the guidelines established in paragraphs 311 through 315 are applicable.

331. PROTECTION OF NAS EN ROUTE COMPUTER SYSTEMS. The primary security concern with respect to the security of NAS en route computer facilities is to minimize the occurrence of any accidental or deliberate event that would affect the operational performance of the online computer equipment. This objective will be accomplished primarily by establishing sufficient physical barriers and administrative controls to prevent personnel not directly associated with the operation or maintenance of the computer hardware, operational software, or facility management from having unrestricted access to the computer equipment areas of each air route traffic control center (ARTCC). Compliance with this standard shall be achieved through local or national adoption of one or a combination of the following physical security alternatives, or the implementation of measures achieving the same objectives:

a. Administrative Controls. The Central Computer Complex (CCC) and Radar Data Processing Room shall be designated and posted RESTRICTED AREAS.

b. Physical Security Alternatives.

(1) Primary entrance doors to the areas shall be secured to prevent access by unauthorized personnel into these areas. Access may be controlled through the use of electro-mechanical locks or other security equipment that facilitate the establishment of access controls. Secondary or emergency doors shall be secured with approved panic hardware.

(2) The use of floor to ceiling partitions within the CCC that will permit continued free flow of personnel through the area to the medical complex, rear exits, and to other floors of the automation wing while preventing uncontrolled access to the computer equipment area.

(3) The adoption of other access control barriers or measures which result from the completion of a formal risk analysis.

332. PROTECTION OF OTHER EN ROUTE FACILITY COMPUTER SYSTEMS. Those ARTCC's, such as Anchorage, Honolulu, and San Juan, which are not part of the En Route Stage A automation project, shall establish adequate physical safeguards for the computer systems in present use commensurate with the guidelines in paragraphs 311 through 318. Upon the installation of new automation equipment, additional physical protective measures will be implemented which conform to those specified in paragraph 331.

333. TERMINAL ATC COMPUTER FACILITIES. The significant differences in site configuration and locations of facilities which house the ARTS II and ARTS III from other important equipment in a typical terminal ATC complex make it undesirable to specify uniform physical security standards for these computer systems beyond those now established for ATC's and TRACON'S in FAA Order 1600.6B. However, the guidelines in paragraphs 311 through 318 shall be considered and utilized as required to enhance security at the facilities. Also, as required by FAA O:der 1600.6B, positive physical access controls to these equipment areas or rooms which house these systems shall be implemented. If the facility is not operational for any part of the day, the equipment area shall be secured to prevent unauthorized entry during periods when the area is not manned or operational.

334. PHYSICAL SECURITY PROTECTION FOR OTHER SPECIAL PURPOSE COMPUTER SYSTEMS. A physical security system conforming to the principles set forth in paragraph 302 shall be established and implemented at other special purpose computer facilities which perform program development, training, or communications switching function in support of the NAS automation programs.

Facilities in this category include, but may not be limited to, ATC computer laboratories at the FAA Technical Center, NATCOM, the Host and ARTS areas at the FAA Academy, and the ARTS area support facilities.

335. ATC SYSTEM REMOTE ENTRY DEVICES. Present and future use of remote access devices with special purpose computer systems requires that a minimum degree of security be given these devices to prevent their unauthorized use.

a. Flight Data Entry Terminals. No additional physical security measures are required provided that the equipment is located in operational areas that are secured in accordance with the provisions of FAA Order 1600.6B.

b. Pilot Self-Briefing Terminal. The possible employment of many remote terminals that may be used as an integral part of the Flight Service Station (FSS) Modernization Program will require the consideration of possible security problems associated with the employment of these devices. Locations selected for placement of FAA-owned terminals shall provide a degree of protection against vandalism of terminal equipment to be used for this program shall be coordinated with the National AIS Security Program Manager to assure that physical security considerations are addressed before operational deployment.

336. PROTECTION OF MAGNETIC STORAGE MEDIA. Data libraries associated with the operation of a special purpose computer facility shall be housed in rooms or areas that provide an adequate level of physical security and environmental protection as specified in paragraph 318. Positive controls shall be implemented to prevent unauthorized personnel from entering these data storage areas. Media storage rooms will be secured after normal duty hours or when access to the area cannot be effectively controlled.

337. SECURITY OF OPERATIONAL SOFTWARE AND RELATED DOCUMENTATION. Master copies of the en route, terminal, and other special purpose operation software shall be placed in secure, fire-resistant storage areas or containers located away from the immediate area of the central computer room. Additional master copies maintained at the Technical Center or an ARTS Area Support Facility shall be accorded similar protection. Documentation files should be accorded adequate protection to prevent deliberate or inadvertent destruction, damage, or loss.

338. - 349. RESERVED.

SECTION 4. ENVIRONMENTAL SAFEGUARDS

350. SCOPE. The contents of this section apply to both general and special purpose computer facilities.

351. FIRE PROTECTION CODES AND STANDARDS. Adequate fire protection for essential AIS systems is achieved through a combination of minimizing the exposure to fire damage by assuring prompt detection and by providing adequate means to extinguish the fire in relation to the type mission and value of the affected computer system. In general, FAA AIS installations shall conform to the standards contained in the National Fire Protection Association (NFPA) Code No. 75, Standard for the Protection of Electronic Computer/Data Processing Equipment, and NFPA No. 70, National Electrical Code. Computer systems installed in buildings under GSA control shall conform to the Federal Fire Council publication, Fire Protection for Essential Electronic Equipment, which has been adopted by GSA as the standard for all GSA facilities. Additionally, FAA AIS installations shall comply with applicable agency and Occupational Safety and Health Administration (OSHA) standards. These standards are identified in Appendix 2.

352. AIR CONDITIONING AND VENTILATING SYSTEMS. Air conditioning systems shall conform to the requirements of NFPA No. 90A, Air Conditioning and Ventilating Systems, and to the additional requirements set forth below.

a. When conditioned air is provided for the electronic equipment area, the air distribution system for that area and associated rooms and repair areas shall be completely separate and independent from any other air distribution system. The refrigeration compressors, circulation system, cooling towers, or similar equipment may, however, be common to other systems.

Exceptions: The requirements above may be modified if the design of the air distribution system prevents the spread of fire, smoke, fumes, etc., from exposing areas into the electronic equipment area. In such cases, fire dampers or fire doors, activated by smoke detection equipment, shall be provided to maintain the fire integrity of the equipment area enclosure.

b. All duct insulation and linings, including vapor barriers and coatings, shall be noncombustible or limited combustible materials.

c. All filters shall meet the requirement of Underwriters' Laboratories, Inc., UL 900, Class I or better, and shall be cleaned or replaced as necessary to prevent dust or lint accumulations.

d. Air ducts serving other areas shall not pass through the electronic equipment areas unless such routing is absolutely necessary and such ducts are effectively encased in fire resistive materials assembled to provide a fire resistance rating equal to that required for the separation walls around the electronic equipment area. Such ducts shall not pass through any special records storage vault or room.

353. ELECTRICAL SERVICE. The requirements set forth below apply to all power and service wiring supplying the electronic equipment area and the equipment. The equipment and inter-connected wiring requirements are set forth in paragraphs 357 through 359.

a. All wiring, including under the floor wiring, shall conform to NFPA No. 70, National Electrical Code. Wiring to electronic equipment shall be fire retardant, and, if run under raised floors, it shall also be water resistant. Communication or other wiring of similar nature under raised floors shall be separated from lighting or power circuit wiring as required by Article 800-3 of NFPA No. 70. If the space below the raised floor is used as a plenum chamber, the installation shall conform to the requirement of Article 300-22. Bundling or stacking of cables in large groups should be avoided. Unused wire or cables shall be removed from the underfloor space.

b. Special attention shall be directed to problem areas involving the use and maintenance of aluminum conductors and terminations. (Reference UL 486 and UL 486B; also see appendix 2.)

c. Building service transformers shall not be permitted in the electronic equipment area. Transformers shall be installed in accordance with the requirements of the National Electrical Code.

d. Rotary electrical equipment such as motorgenerator sets or emergency generation equipment shall not be permitted in the electronic equipment area. Rotary electrical equipment shall be installed in accordance with NFPA No. 70.

e. In conjunction with the electrical source, surge conductors should be incorporated into the system to minimize fluctuations in the electrical current.

f. Isolate computers from power sources used by major appliances or other office equipment.

354. EMERGENCY SHUTDOWN CONTROLS.

a. A prominently labeled master control switch(es) shall be located at each principal exit to the electronic equipment area. These switches shall disconnect power to all electronic equipment. These master control switches shall be in addition to any emergency shutdown for individual machines or other units of equipment.

b. Switches shall be provided at egress points from the electronic equipment area to permit the shutdown of air handling equipment. Manually activated exhaust and ventilating systems shall have startup and shutdown switches at the egress points.

355. UNINTERRUPTABLE POWER SUPPLIES.

a. Solid state equipment or motorgenerators, including associated switchgear, inverters, rectifiers, batteries, and all other components of an uninterruptable power supply, shall be installed in accordance with NFPA No. 70.

b. All uninterruptable power supplies shall be provided with fire protection systems in accordance with paragraphs 362 through 369 according to the criticality of the electronic equipment which is being served.

356. OTHER UTILITIES. Chilled water piping, domestic water supplies, sanitary drains, roof drains (rain), gas lines, fuel oil lines, steam lines, water mains, and other utility lines not serving the electronic equipment area shall be prohibited from the electronic equipment and record storage areas.

357. EQUIPMENT. The use of combustible materials, particularly plastics for wire insulation, printed circuit boards, and other components, as well as the necessary internal configurations of electronic equipment, can, under normal operating conditions, support combustion to a degree sufficient to cause serious internal damage. Examination of the history of fires in electronic equipment, and those combustible materials essential to equipment design shows that, once started, combustion may continue until extinguished or until it totally damages the compartment or origin with a potential for spreading to other compartments. It is the intent of these requirements to mitigate fire development and propagation by reasonable criteria that will limit the amount of combustible material and provide barriers against fire propagation to the degree consistent with the operating needs of the equipment. Therefore, specific combustibility classifications are not aligned to electronic equipment. Any equipment not conforming to the recommendations of this chapter may present risks to itself and/or to neighboring elements greater than that which is necessary or should be tolerated.

358. OPERATING ENVIRONMENT. The quantity of combustibles permitted within the computer rooms shall be kept to an absolute minimum. These requirements will not only reduce the possibility of a fire but also limit the severity of any fire, should one occur.

359. REQUIREMENTS. Storage of excess printout paper, tapes, records, file cabinets, and packaging materials shall not be allowed in the computer room. Within the computer room, the storage of all combustible supplies shall be restricted to the minimum level required for efficient day to day operations, and these materials shall be kept in totally enclosed metal containers or file cabinets. Storage rooms outside the computer room shall be provided for reserve stocks for supplies, including paper, magnetic tapes, and other items required for continuing operations.

a. All office furniture in the computer room shall be kept to a minimum and shall be of metal construction or of other materials that do not contribute significantly to the combustible contents. Coatracks shall not be permitted in computer rooms, as they contribute an unnecessary additional fuel source, as well as undesirable traffic, dust, and lint conditions.

b. Small supervisory office areas and similar light hazard occupancies directly related to the computer room operations may be located within the computer room, provided all furnishings are metal and adequate facilities are provided for containing the necessary combustible materials. Paper or other combustible materials shall be strictly limited to that needed for efficient operations.

c. Waste containers shall be made with a self closing feature or flame suppressing design and shall be emptied periodically so as to prevent an overflow. As a minimum, all waste containers shall be emptied at the end of each workday.

d. All aisles, exits, and exit markings shall conform to the Life Safety Code, NFPA 101. At no time shall materials or equipment be placed in any manner which restricts the aisles or exits.

e. Materials used for acoustical treatment shall conform to the construction requirements of paragraph 312 b.

f. Smoking, eating, and drinking shall not be permitted in computer rooms. Signs stating such restrictions should be posted at each entrance and ashtrays placed outside each entrance.

g. Only authorized persons shall be permitted in the computer room and associated work areas. Notice of this restriction should be posted at each entrance. Traffic into the computer room should be kept to a minimum.

h. The following are prohibited in the computer room:

(1) Any activity, electric appliances, or occupancy not directly associated with the electronic system(s) involved.

(2) Storage of office supplies, forms, stationery, and other combustible supplies.

(3) Components of the computer operation which are neither electronically interconnected to the essential system nor required in close proximity and either:

(a) Involve the presence of large quantities of paper or other combustible material, or

(b) Contain significant amounts of combustible material, such as wire insulation, combustible housing, etc., or

(c) Are in themselves critical to the operation and would require a long lead time to replace. (Such equipment shall be contained in a fire resistive cutoff area of its own with such fire protection as is appropriate.)

(4) Maintenance shops and maintenance operations, except for those repair and maintenance operations which must be performed directly on equipment which is impractical to remove from the electronic equipment area.

(5) Bulk storage of records.

(6) Any other combustible material, equipment, or operation which constitutes a hazard and which can be removed.

(7) Unpacking, uncrating, or storage of equipment.

(8) Traffic of machines, material, or personnel through the equipment area.

i. Computer rooms which require the processing or use of recording materials, such as magnetic tapes, magnetic discs, punched cards, or printout paper, shall provide uniquely identified space for the input and output staging and handling of these records. This area shall be in addition to that required for equipment aisles, entrances, and exits, and separated by a fire resistant wall whose rating is at least 1 hour.

360. <u>FIRE PROTECTION SYSTEM</u>. Important elements of a fire protection system provide for the detection of a fire situation and manual or automated response to extinguish the fire. Neither capability is of any service without the other. It should further be realized that the occurrence of a fire of any magnitude constitutes a loss even though that loss is of negligible value (such as a waste fire). Of primary importance upon detection of a fire situation is to locate and identify the source or area of concern and extinguish the fire.

The anticipated chronology of the action in a computer room or record storage area constructed, protected, and operated as required herein is:

a. Detection of a fire situation by the early warning smoke detection system or the occupants;

b. Activation of the facility emergency plan for which portable extinguishing equipment is available for manual first aid response;

c. Optional automatic use of Halon 1301 gaseous agent to extinguish the fire; and

d. Protection from disastrous loss through activation of the automatic sprinkler system in areas where there has been a high heat release.

The protection system set forth below provides the capabilities to detect and extinguish fires, as well as to protect against a major disaster. (See figure 3-2, Quick Reference Chart, for a summary of required protection).

361. AUTOMATIC SPRINKLERS. The purpose of automatic sprinklers is to provide disaster protection by limiting and controlling major fire incidents and preventing total destruction of the computer room or records. Sprinkler protection is designed to prevent a fire from progressing beyond control and developing into a disaster involving total destruction of all equipment and records in the area, and backs up other extinguishing media, manual and automatic, which may be employed.

This backup is required due to the characteristic dense, acrid smoke conditions and the inaccessibility of the facility even to professional firefighters when confronted by a significant plastics (cable insulation, electronic components, tapes, etc.) fire.

a. Automatic sprinkler protection is required for all computer rooms and record storage areas. It shall be installed in accordance with NFPA No. 13, Sprinkler System. Each automatic sprinkler section covering a computer room or record storage area shall be provided with a water flow alarm. The alarm will sound locally and shall also be connected to the local fire department or to an approved central station supervisory service. The sprinkler system may be valved independently from other sprinkler systems. The zone valve shall be equipped with electrical supervision.

b. Sprinklers for computer room spaces shall be designed on a basis of 0.075 gallons per minute per square foot over the most remote 3,000 sq. ft. of area. For areas less than 1,500 sq. ft., design density shall be 0.1 gpm/sq. ft. Sprinklers for tape libraries with storage racks no higher than 8 ft. and having no substantial concealed space shall be designed on the basis of 0.2 pgm/sq. ft. over the most remote 1,500 sq. ft. (Ref. NFPA 13, Sprinkler Systems).

c. There are many types of sprinkler systems. Each system presents various options and benefits to the user. The basic requirement stated in this section is to provide automatic sprinkler protection. The typical "wet pipe" standard system is effective and the least expensive of the automatic sprinkler systems. A wet pipe system designed as specified herein is acceptable. Local conditions, particular installations, and management concerns may determine the need for additional sophistication in the design of the automatic sprinkler system for use in their facility. Use of on/off sprinkler heads, pre-action systems, or dry pipe systems are a few of the options available to minimize the quantity of water usage by requiring concurrent multiple detection prior to discharge, or eliminating water from the piping unless required for discharge. Systems which rely upon manual activation are not acceptable. Any automatic sprinkler system shall be engineered for the specific area to be protected, utilizing the design constraints of NFPA #13, and meet all the requirements of this section.

d. Some electronic system components, such as cotton braid covered and/or paper insulated wires and cable found in older telephone equipment, are more susceptible to water damage than those manufactured with newer plastic technology. In these situations, special consideration should be given to on/off sprinklers and/or other systems designed to minimize the quantity of water used.

e. For the protection of trailers, totally unmanned and remote installations, arctic installations, or the like, where there is no water supply to support the operation of an automatic sprinkler system, a Halon 1301 total flooding system shall be provided. All Halon 1301 installations of this nature shall have a 100 percent connected reserve supply of Halon 1301.

362. AUTOMATIC SMOKE DETECTION EQUIPMENT. The purpose of automatic smoke detection equipment is to minimize losses resulting from a fire by: (a) alerting operational personnel who can make use of portable fire extinguishers prior to the operation of automatic extinguishing equipment, (b) summoning the fire department, and (c) serving as the initiator of controls for special extinguishing systems, air handling shutdown, etc.

a. Design and installation of this equipment is subject to a great many variables. Some of the important considerations which have major impact upon the design and use of automatic smoke detectors are:

(1) Air currents and patterns (rooms, plenum, areas, etc.).

(2) Control of power to equipment.

(3) Control of air handling equipment.

(4) Prevention of removal of gaseous extinguishing agents at the time of their discharge by air handling equipment.

(5) Continued use of area internal air circulating systems to promote and assist rapid dispersal of gaseous extinguishing agents.

(6) Control of the discharge of total flooding. Halon 1301 extinguishing systems.

(7) Compatibility with existing systems with which interconnection is to be made.

b. Automatic smoke detection equipment capable of early warning detection shall be installed in all computer rooms and record storage areas. The equipment used shall be a listed smoke detection type. Each installation shall be engineered for the specific area to be protected and meet the requirements of NFPA No. 72E, Automatic Fire Detectors. The detector system shall be connected to an alarm which will sound locally and will relay the alarm automatically to the local fire department or to an approved central station supervisory service.

c. Contracts for detection systems and interconnection with electrical switch gear shall include provisions for acceptance tests using performance criteria and conditions present in a real fire.

363. PORTABLE FIRE EXTINGUISHING EQUIPMENT. The purpose of locating portable fire extinguishing equipment immediately available to operations personnel and others is to provide the capability of controlling small fires in electronic equipment areas. Class A extinguishers provide extinguishing capability for ordinary combustibles (paper, wood, cloth, plastics, etc.) in the form of paper and magnetic tape records, logs, worksheets, interior finishes, decorations, machine components, etc. Class C extinguishers provide extinguishing capability when electrical energy is involved. Generally, electrical energy-induced fires in areas within the scope of this document will involve Class A type ordinary combustible materials.

a. Every computer room and record storage area shall be provided with Class A and Class C fire extinguishers prominently located within the space so that an extinguisher is available within 50 feet of travel of any part of the space. The following requirements apply:

(1) To combat a Class A fire, a listed Class A fire extinguisher of the pressurized plain water type with a minimum rating of 2A must be available. To be effective, this extinguisher must be located within 50 feet of any part of the area that it is designated to protect.

(2) To combat a Class C fire, a Halon 1211 handheld extinguisher with a minimum rating of 10BC and 5LB capacity must be available. To be an effective tool, this extinguisher must be located within 50 feet of any part of the area that it is designated to protect.

(3) A sign shall be located adjacent to each portable extinguisher plainly indicating the type of fire for which the extinguisher is intended.

b. All portable fire extinguishers shall be installed, maintained, and used in accordance with the requirements of NFPA No. 10, Installation, Maintenance and Use of Portable Fire Extinguishers, and FAA Order 6930.1A, Fire Prevention and Maintenance of Fire Protection Equipment. The fire extinguishers shall be readily accessible at all times.

c. Hose Lines.

(1) In installations where conditions may require the provision of inside water hose, it shall be equipped with shutoff and combination solid stream and water spray nozzle.

(2) In installations where conditions may require the provisions of carbon dioxide hand hose lines, they shall be installed and maintained in accordance with NFPA No. 12, Carbon Dioxide Extinguishing Systems.

364. MANNED RESPONSE. The activation of the detection system can have no benefit unless a response takes place. The availability of people to respond to an alarm may mean the difference between a major or minor loss. The speed with which this response takes place is the principal variable. The purpose of this section is to highlight the integral importance of providing a manual response effort as a part of the overall fire protection system. Paragraph 381, Emergencies, outlines the requirement, purpose, and duties of an emergency control organization. The response of this emergency control organization utilizing the fire fighting equipment provided may (a) detect and extinguish a fire prior to activation of the smoke detection system, (b) ascertain the location, assess the condition, and extinguish the fire, and (c) sense impending danger and take preventive measures, all of which can limit the extent of damages or loss to a very small amount.

a. Normal operations periods (regular shifts, high or maximum number of people). Provisions shall be made for an emergency control team during normal operations periods. With many personnel in or about the area, the problems faced in organizing and maintaining this team are not as complex as might be required during the off-shift period described below.

b. Off-shift periods (midnight shifts, weekends, holidays, minimum manning periods, and maybe coupled with major facility modifications). Of equal if not greater importance than the normal operations period is the provision for an emergency control team during a slack or off-shift period. Though this team may not be structured like, nor composed of, similar numbers or skills of people, it is during these off-shift periods that the greater need exists. (Statistically, the greater proportion of fires that develop into major losses begin during off-shift periods.) Management must carefully evaluate the minimum periods of staffing (no matter how infrequently they occur) and shall provide an adequate emergency control team.

c. In summation, an emergency control team meeting the requirements of paragraphs 379-384 shall be provided at all times, day and night, prime and off-shift. The size, structure, and duties of the individual shift teams may vary between shifts, but their duties and responsibilities shall conform to the requirement of paragraphs 379-384.

365. HALON 1301 SYSTEMS.

a. The purpose of including Halon 1301 systems is to provide the option of using the Halon extinguishing agent for extraordinary situations. Whenever a Halon 1301 system is used, it shall be in addition to the requirement for automatic sprinklers, automatic smoke detection equipment, portable fire extinguishing equipment, and manual response. When a Halon 1301 system is used, consideration must be given to the provision of exhaust ventilation to remove the Halon vapors after a fire. (Exception - See paragraph 363.e.) Halon 1301 systems may be considered in computer rooms where there is:

(1) Critical need to protect data in process,

(2) Desire to reduce equipment fire damage through early automatic fire extinguishment.

(3) Need to protect void spaces not suited for sprinkler protection (for example, beneath the raised floor areas), and

(4) Critical need to facilitate return to service.

b. When a Halon 1301 system is selected for the protection of electronic equipment areas, it shall be installed in accordance with NFPA No. 12A, Halogenated Fire Extinguishing Agent Systems - Halon 1301. No system shall be installed which requires a design discharge density of more than 7 percent. Unnecessary exposure of personnel to the agent or to the decomposition products caused by a fire should be avoided.

c. Each Halon 1301 system shall be provided with a discharge alarm which will sound locally and will be connected to the local fire department or to an approved central station supervisory service.

d. Automatic Halon 1301 systems shall be activated by an automatic early warning detection system meeting the requirements of NFPA No. 72E, Automatic Fire Detectors. The same Automatic Fire Detection System required by paragraph 367c may be used to satisfy the requirement of this paragraph. However, any automatic fire detection system used shall meet the requirements of paragraph 364 and all subparagraphs.

e. The automatic detection system shall:

(1) Be interlocked to shut down any air handling equipment which would exhaust the Halon 1301 agent upon discharge, and

(2) Initiate a minimum of 20 second delay between the sounding of the alarm (detection of fire) and discharge of the Halon 1301 agent.

Note 1: The delay is provided for the evacuation of personnel and cycle-down time for the air handling equipment.

Note 2: It may be desirable to continue internal circulation fans for improved distribution and mixing with air of the Halon 1301.

Note 3: The use of a detection system arranged to provide cross-zoned, dual detection prior to discharge may be advisable to activate alarms, time-delay devices, and minimize discharge of the agent and exposure of personnel. For example, a cross-zoned detection system might initiate the following sequence: (a) first-zone detection - immediate audible alarm; initiate automatic time delay; initiate automatic shutdown of external air handling equipment; evacuate personnel; emergency team locate and confirm alarm source; permit manual override; conduct first aid; initiate fire extinguishment; (b) second zone detection - automatic confirmation of or wait for completion of design time delay; discharge Halon 1301 agent.

f. When a Halon 1301 system is employed, provision shall be made to vent the Halon to the outside after discharge without contaminating the entire facility. Opening outside door may suffice, possibly assisted by portable fans. Some inaccessible areas may require more elaborate means for Halon removal. The exhaust ventilation system noted in paragraph 367a may be appropriate.

g. All contracts for the installation of Halon 1301 systems shall include provision for performance and acceptance test utilizing actual discharge and agent concentration profile determination following the completion of the installation. The discharge shall be activated by the detection system required by paragraph 367e.

h. An open purchase order shall be provided, authorizing the recharge of the Halon 1301 system immediately, each time it is discharged, without further negotiation.

i. No other fixed extinguishing system which exhibit fire extinguishing abilities such as other Halons and carbon dioxide can be recommended. Use of any of these other systems is expressly prohibited without careful study and evaluation to determine and resolve their significant hazard to life and health.

366. RAISED FLOOR AREA PROTECTION. The space under a raised floor presents a significant additional problem and hazard to the computer operation and warrants separate consideration. Accumulations of cables, dust and/or dirt, and possible other combustible (paper, cards, etc.) require protective measures. The greater the depth of the raised floor area, the greater the potential for hazard. In addition to construction of the raised floor in accordance with the requirements of paragraph 314b, protection shall be provided in accordance with the following subparagraphs:

a. An automatic smoke detection system meeting the requirement of paragraph 362 shall be installed under all raised floors. This automatic smoke detection system may be a part of the same system used for the equipment area or may be a separate system. In either case, detection system zoning shall provide for a clear and distinct indication of a detection originating in the under-floor space.

b. Floor lifting devices shall be installed and maintained in readily accessible locations throughout the computer room and/or record storage areas. The floor lifting devices installed shall be of the style appropriate to grasp the floor covering material used in the installation (see paragraph 314b (6)). A floor lifting device shall be available within 50 feet of travel of any part of the area.

c. Any raised floor whose depth is under 18 inches may be protected with an automatic Halon 1301 system meeting the requirements of paragraph 365. When an automatic Halon 1301 system is used beneath a raised floor area, automatic smoke detection system required by paragraph 368a shall be the activation source for the discharge.

d. Any raised floor area whose depth is between 18 and 36 inches shall be protected with an automatic fire extinguishing system. The system may be an automatic sprinkler or automatic Halon 1301 system meeting the requirements of paragraph 361 or 365. When an automatic Halon 1301 system is used beneath a raised floor, the raised floor area automatic smoke detection system required by paragraph 366a shall be the activation source for the discharge.

e. Any raised floor area whose depth exceeds 36 inches shall be protected with an automatic sprinkler system meeting the requirements of paragraph 361 and all subparagraphs.

367. SPECIAL PROTECTION SYSTEMS. Special protection of individual systems, or parts of a system which constitute an exceptional value, hazard, or risk, may be desirable. The form that this protection takes is too wide and varied for an in-depth discussion here. The options include, but are not limited to, installation in a vault or vault like structure, inert gas flooding the unit or the unit and the area about it, and inclusion of an automatic fire extinguishing system within the unit. An example of systems which might fall into this special or exceptional category are mass memories or one of a kind electronic control units.

a. When an area of special consideration is involved, the protection for that area or system should be specially engineered for the application, activity, and risks present by a team composed of electronic systems engineers and fire protection engineers.

368. GENERAL STORAGE. Normal computer operations may involve storage of sizable quantities of combustible materials. Printout paper, stationery supplies, unused magnetic and paper tapes, packaging materials, and other types of combustible supplies are customarily stored. If not rigorously controlled, the storage of these items may become a serious fire hazard. An accumulation of supplies should be clearly recognized as fuel load for potential fires which might damage costly electronic hardware and destroy valuable records.

a. The presence of all combustible supplies within the computer room shall be restricted to the minimum level required for efficient day to day operations, and these materials shall be kept in totally enclosed metal containers, cabinets, or files.

b. Storage rooms outside the computer room shall be provided for reserve stocks of supplies, including paper, magnetic tapes, and other items required for continuing operations.

369. RECORDS. Some computer installations involve the creation, use, and storage of large quantities of input and/or output records. These records in some instances can be more important to continuity of operations than the computer equipment itself. Requirements for protection of records on paper-based materials are derived from extensive experience with paper in fire situations and long-established standards. Protection needs of records on plastic-based materials were determined from limited experience and knowledge. It is known that plastic-based materials are more susceptible to fire damage than paper-based records and that protection methods sufficient to safeguard paper records are less than adequate for plastic-based materials.

a. Typical recording media include punch cards, plastic- or metal-based electronic tapes, paper or plastic punch tapes, microfilm, and other photographic media. Control panels, magnetic discs, memory drums, memory cores, semiconductors, monolithic core, and laser or bubble memories are other media for data storage in machine-usable form. When these media are used to record information in a form removable from the computer room and the equipment area, the problem of record storage develops.

b. Storage devices involve a wide range of configurations designed to hold specific kinds of data in a computer assembly. Each device must store data in an arrangement compatible with the computer in use. Protection of storage devices, therefore, concerns safeguarding the data which are loaded into the unit and its capability to function properly. When a storage device such as a drum, magnetic core, mass storage, or disc file is permanently mounted within the computer system, the fire protection required shall be equivalent to that prescribed for the equipment area. When, however, these devices do not remain permanently mounted within the equipment on which they are used, they shall be stored in containers appropriate to their physical protection. These storage devices shall be categorized and protected as required in the following paragraphs (see paragraphs 370 and 371).

370. RECORD CLASSIFICATIONS. The degree of protection provided records shall be directly related to their importance. In this context, importance will be measured by an evaluation of what the loss of a particular record would mean in terms of accomplishing the mission of a computer system and reestablishment of operations after a fire. To maintain a reasonable sense of consistency, it should be assumed that computer equipment capable of properly processing input records will be available. The following method for categorizing all records is based on their relative importance to the established mission and their after the

fire value. This method prescribes that all records shall be evaluated and assigned to one of four general classes. It simplifies the problem of safeguarding, assuring adequate protection is provided where required and superior protection is not used unless warranted. The adaptation used is that originated by the NFPA Committee on Electronic Computer Systems in their standard NFPA No. 75, Protection of Electronic Computer/Data Processing Equipment, and is based upon NFPA No. 232, Protection of Records.

a. Class I (Vital) Records. Records that are essential to the mission of the equipment, are irreplaceable, or would be needed immediately after the fire and could not be quickly reproduced. Examples might include key programs, master records, equipment wiring diagrams, and certain input/output memory data.

b. Class II (Important) Records. Records that are essential or important, but which, with difficulty or extra expense, could be reproduced without a critical delay of any essential missions. Some programs, wiring diagrams, memory, and input/output data have this level of importance.

c. Class III (Useful) Records. Records whose loss might cause much inconvenience, but which could readily be replaced and which would not be an insurmountable obstacle to prompt restoration of operations. Programs and procedures retained as examples of special problems are typical of records in this category.

d. Class IV (Nonessential) Records. Those records which on examination are found to be no longer necessary.

371. RECORD PROTECTION. The means of protection to be utilized for records are described here.

a. Duplication of Records. The surest method of safeguarding records consists of duplicating and storing copies in an area separate from the originals. This normally assures that the two sets of records will not be subjected to damage from the same fire. In some electronic installations, duplication of records in the same or different media is a common practice.

b. Vaults.

(1) The term "vault" refers to a completely fire-resistant enclosure to be used exclusively for storage. NO WORK IS TO BE PERFORMED IN THE VAULT. The vault is to be so equipped, maintained, and supervised as to minimize the possibility of origin of fire within and to prevent entrance of fire from without.

(2) The construction shall be as specified in NFPA No. 232, Chapter 2, and is intended to provide not only a factor of safety for structural conditions, but also (a) to prevent the passage of flame or the passage of heat above a specified temperature into the vault chamber for a stated period, and (b) to permit withstanding the stresses and strains due to the application of a firehose stream while the unit is in a highly heated condition without materially reducing its fire resistance. On the basis of the foregoing, vaults are classified as "6-hour," "4-hour," or "2-hour."

c. Record Protection Equipment. Record protection equipment is movable equipment intended to segregate records from surrounding exposure and hazards and is classified in terms of an interior temperature limit, a relative humidity limit, and a time in hours. Only Class 150 F-85 percent relative humidity record protection equipment is acceptable for use within the scope of this standard. The Class 150 record protection equipment description and specification is as included in NFPA No. 232, Chapter 4.

d. Closed Metal Files and Cabinets. Closed metal files and cabinets, i.e., general metal office equipment, are not generally rated for their ability to protect from or resist the effects of a fire. However, in essential electronic equipment areas already protected according to the requirement of this standard, these files and cabinets offer a degree of isolation and protection from physical contact which is of acceptable benefit. Therefore, the use of nonrated, closed, and of metal construction files and/or cabinets is acceptable in accordance with the limitations of paragraphs 371e and f.

e. Protection of the Records. Standard practice for the protection of Class I (Vital) and Class II (Important) records shall require duplication of the records. For Class III (Useful) duplication is optional and for Class IV (Nonessential) duplication is not required. Each copy of the records shall be stored in a separate fire area.

Exception: For Class I (Vital) and Class II (Important) records, it is recognized that there are types of records and situations where duplication is not possible or is ill-advised (for example, cryptographic information, highly sensitive data, or information protected by the Privacy Act). In these circumstances, a record protection vault shall be constructed. The vault shall be constructed as required by paragraph 373b and shall have a minimum 4-hour rating. In high hazard areas, a 6-hour rating shall be used.

After the duplication of the records, one of two conditions exists:

(1) (The preferred condition) - each of the two or more copies has been removed from the computer room. For this condition, the requirements of paragraph 371 f(1) apply to each copy;

(2) (The other condition) - for operational considerations, one of the copies remains within the computer room and one copy is removed to a separate area. For this condition, the requirements of paragraph 371f apply to each copy which has been removed from the equipment area and 371g applies to the copy retained within the computer room.

f. Protection of Records Stored Outside the Electronic Equipment Area. To the maximum extent consistent with efficient operations, all records shall be stored outside the computer room. Adjacent, properly protected records, or tape libraries which may open directly into the computer area are acceptable providing they have been constructed in accordance with the requirement of paragraphs 312 through 315 and are protected in accordance with paragraphs 361 through 367.

(1) In a Record or Tape Library. When more than one record or tape library is provided, one of these shall be in a totally separate fire area. Both record or tape libraries shall be constructed in accordance with section 2 and protected in accordance with paragraphs 361 through 367.

Class I (Vital), Class II (Important), Class III (Useful): These categories of records on metal based materials, plastics, or paper, if duplicated and stored separately as required above, require no special protection when housed in a records or tape library meeting the requirements of this paragraph.

Class IV (Nonessential) records shall be held to a minimum. Provisions shall be made for their quick and easy disposal according to a known retention plan. No special protection requirements apply to nonessential records.

(2) When a Record or Tape Library is Not Provided. In certain situations, the type of computer system does not involve a large enough quantity of records to make it economically feasible to construct record or tape libraries. These situations should be carefully evaluated and treated as the exception to the rule. In these situations only, the following standards apply:

Class I (Vital) and Class II (Important) records shall be duplicated. One copy of each record shall be stored in a Class 150 4-hour rated record protection device, (ref. paragraph 373c), which may be located adjacent to or near the computer room. The other copy shall be in a separate fire area, preferably in a separate building but at least in an area remote from the computer room, and the copy contained in the Class 150 4-hour rated device required above.

Class III (Useful) records, if not duplicated, shall be stored in Class 150 2-hour rated record protection equipment (ref. paragraph 371d).

g. Protection of Records Stored Within the Computer Room. The quantity of such records shall be kept to the absolute minimum required for immediate use.

Class I (Vital) and Class II (Important). The copy remaining with the area shall be stored within Class 150
1-hour rated record protection equipment (ref. paragraph 371c).

Class II (Important) records of paper- or plastic-based materials shall be stored with totally enclosed metal files or cabinets (ref. paragraph 371d).

Class III (Useful) records on metal-based materials require no special protection.

Class IV (Nonessential) records shall be prohibited from storage within the computer room.

372. PROTECTION OF COMPUTER SUPPLIES. Computer supplies are the most combustible materials used in a data processing installation. Consequently, the most ideal solution to the threat posed by these paper stocks is to store as few as possible in the computer facility itself. A central storage location which is as fire resistant as practical should be utilized. This can be equipped with suitable fire alarms and extinguishing systems, if deemed appropriate, after such factors as value, criticality to operations, and proximity to central computer complex are considered.

373. LOCAL FIRE FIGHTING SUPPORT. The manager of each computer data processing facility should assure prompt, adequate procedures have been established to obtain local fire fighting assistance. This should include provisions for adequate alarm and communication procedures, and assuring that the people who work in the computer room are familiar with fire contingency plans and know what to do should a fire occur. Where practical, local fire department officials should be invited to visit the facility, review the fire protection system being utilized, and discuss with appropriate personnel matters involving fire protection of the computer facility.

374. FIRE PROTECTION OF REMOTE TERMINAL AREAS. Rooms selected for use as remote terminal facilities should be provided with an appropriate number of portable fire extinguishers suitable for use in both electrical and paper fires. Consideration may be given to the installation of smoke or ionization detectors in the event such equipment is operational or energized after normal duty hours.

375. PROTECTION AGAINST WATER DAMAGE. More insurance claims are received from DPA's as a result of water damage than any other source. Below ground or basement sites are particularly vulnerable to flooding from backed up sewer lines, broken water mains, heavy rain, and swollen streams. If such a site is utilized, provisions should be made for drains, pumps, and emergency power for pumps. No matter where the computer installation is located, a fire on the floor above will result in an excessive buildup of weight and water that may produce leakage into the facility. The use of drains, bunkers, and channels will alleviate potential problems of this nature, as the floor to floor integrity designed into a building is often lost by drilling holes for utilities. These holes should be sealed to prevent their use as a path for fire or water. One additional protection against water damage is the use of plastic sheeting to cover vital pieces of equipment. This can be used to protect against ruptured pipes and water leakage from the floor above, after the equipment has been de-energized. Plastic covers should be removed promptly when no longer required so as to prevent excessive heat buildup. The covers must be removed before the equipment is re-energized to avoid damage due to heat.

376. PROTECTION OF SUPPORTING UTILITIES. Every AIS facility is dependent upon supporting utilities; electric power, air conditioning, and other essential services, such as communications circuits and water.

a. Building or room housing uninterruptible power supplies shall be protected in accordance with the requirement established in FAA Order 1600.6B. All doors will be of solid construction and equipped with the FAA locking system. Any windows or large openings which can be used as a point of access shall be barred or screened to preclude surreptitious entry. Fuel tanks used to support emergency power sources should also be protected to the extent possible.

b. Other electrical facilities which support computer systems such as electrical closets and transformer vaults shall be secured with the agency locking system.

c. Terminal boards and other communications equipment associated with teleprocessing computer system shall be located in locked rooms to which access is strictly controlled. Consideration shall also be given to the vulnerability of power and communication cabling in manholes, ducts, etc.

377. PROTECTION AGAINST THE EFFECTS OF MAGNETISM. While the hazard to magnetic computer storage media from magnets has received significant attention, far beyond the real potential threat, possible disruption or damage to storage media from this source cannot be totally discounted. To provide maximum protection against the effects of magnets, all magnetic storage media containers will be kept at least 20 inches away from an exterior wall. This can be accomplished in the tape/disc library by maintaining a walking corridor around the room perimeter. Consideration should also be given to the adverse effects of magnetic media near conduits that could serve as a conductor of lightning discharge currents.

378. ELECTROMAGNETIC RADIATION. The hazards posed by electromagnetic radiation to computer equipment operations and magnetic storage media have received undue attention when compared to the actual threat.

a. Equipment Operations. There have been instances of strong radar signals causing instantaneous computer errors when the computers were placed in the direct path of the radar facility. While such a situation could occur at an air traffic related facility, the problem can be overcome by grounding the metal work in the facility or erecting a grounded metal screen.

b. Storage Media. There is little hazard from external radiation to data stored on tapes or discs.

379. GENERAL EMERGENCIES. Emergency operations include the establishment of programs for firefighting and other self-protection organizations, salvage procedures, arrangement for continuance of operations after fires, and programs for the replacement of destroyed records.

380. EMERGENCY ORGANIZATION. An emergency control organization shall be established. The following paragraphs describe functions which should be included in such organizations but do not attempt to dictate the exact organization. Each facility must determine its individual best method of providing the needed protection.

a. The purpose of the emergency plan shall be to:

(1) Prevent or minimize danger to life and to prevent injury.

(2) Prevent or minimize damage to electronic equipment.

(3) Prevent or minimize danger to vital and important records.

(4) Preserve the ability of the computer equipment to perform its missions.

(5) Prevent or minimize damage to other operations and equipment.

(6) Prevent or minimize damage to the building housing the operation and other buildings in the area.

b. Emergency teams should be organized and trained to use the available manual, hand operated, or portable firefighting equipment to combat incipient fires. While the training of the emergency teams should be complete, it is of prime importance that every person working in the computer room know how and when to use emergency shutdown controls, any fixed fire protection, and the portable fire extinguishers. The duties of the emergency teams should include:

(1) Ascertaining that the fire alarm has been activated and the fire department has been called.

(2) Assuring the evacuation of personnel from any area of fire danger.

(3) Directing emergency shutdown of computer equipment and utilities. Building lighting should not be shut down.

(4) Conducting firefighting operations as long as conditions are tenable, reasonably safe, and within the capabilities of the protective equipment provided.

(5) Directing the fire department to the scene of the fire and standing by to aid the fire department and provide information.

(6) Directing the removal of portable equipment and records endangered by the fire.

(7) Informing management of the incident and extent of loss and damage.

CAUTION: Fire fighting efforts shall only be made by FAA employees where there is reason to believe that a fire can be brought under immediate control. In all cases, safety and egress of peronnel are of paramount importance and shall not be jeopardized by fire fighting efforts.

381. PRACTICE AND DRILLS. The duties of the emergency teams require considerable planning and training. In addition to being trained in the effective use of various types of emergency equipment, it is essential that practice drills be scheduled periodically. Following each drill or exercise, a critique should be conducted which includes a review of the entire operation. Each member of the emergency team should know which equipment and records are the most important and should receive the first attention in case of fire. Team members should be provided with proper protective clothing and respiratory protection.

382. SALVAGE OPERATIONS. Immediate action is the key to successful salvage functions. In the event of a fire with a resulting spread of smoke or use of water, prompt salvage operations can aid greatly in rapid restoration of operations and limitation of damage. Adequate planning is necessary to ensure prompt action.

a. Where water may be used on the floor above to fight a fire, or there are other water sources above the computer room, means should be provided to prevent the water from entering the equipment. Waterproof covers should be provided and stored at some convenient location for just this type of emergency. In some instances, temporary shielding can be obtained by taking off the side covers of equipment and placing them on top of the exposed units.

b. Whenever electronic equipment has been doused with water, firefighting chemicals, smoke, or soot, it is imperative that action be taken to clean and dry the equipment as soon as possible. If clean water has been the contaminant, drying is all that is required. Otherwise, cleaning before drying is necessary. Failure to treat or remove contaminant promptly may greatly increase damage.

c. A supply of water displacing compound should be available so that emergency treatment of damaged equipment can begin as soon as the fire is out.

CAUTION: The water displacing compound may be flammable at room temperature. If so, all sources of ignition, such as pilot lights, etc., should be turned off and appropriate safeguards taken. In addition, avoid inhaling the vapors of the compound as they may be injurious to health. Both of these precautions should be prominently displayed on the container but, in the event they are not, be guided by the above cautions.

(1) When equipment is contaminated with dirty water, firefighting chemicals, or smoke and it cannot be cleaned within 24 hours after contamination, corrosion and deterioration may be reduced by means of an emergency treatment. This consists of washing as much soot, smoke, and/or firefighting chemicals as possible from the equipment with a medium pressure water spray. The wet equipment should then be sprayed with a protective coating type water displacing compound and allowed to dry.

(2) Clean, wet equipment can be dried by spraying the wet equipment with a noncoating type water-displacing compound and then blowing the equipment with warm air to evaporate the mixture of water-displacing compound and water.

(3) Good ventilation is necessary for these operations.

d. All personnel involved in the salvage operation shall be aware of the location of waterproof covers, mops, brooms, squeegees, water displacing compounds, immersion pumps, vacuums, and other equipment useful in the reduction of water damage.

383. DISASTER CONTINGENCY PLANNING FOR RECOVERY AND REESTABLISHMENT OF OPERATIONS. The prompt reestablishment of operations after a damaging fire, flood, or other disaster depends on the availability of alternate equipment which can be used to perform the function of destroyed equipment, the ability to replace or restore the damaged equipment or records, and the restoration of any damaged facility or of the ability to use an alternate area for substitute equipment, as follows:

Plan Items	Consideration		Options
Equipment	Alternates	(1)	Prepared agreements w/duplicate facilities
Facilities	Restore	(2)	Duplicate records for facilities
Records, single copy (paper)	Replace	(3)	Plan for restoration copy records

384. TRAINING FOR EMERGENCIES. It is of cardinal importance that all personnel involved in the operation of essential computer equipment be thoroughly trained in how to notify the local fire department of a fire, and the use of all the firefighting equipment available within or adjacent to the operating area. Furthermore, the personnel should all be thoroughly familiar with the procedures required in the event of a fire, in addition to the capabilities and limitations of the firefighting equipment available to them, i.e., power shutdown switches, smoke exhaust systems, etc.

a. After initial training and orientation with the fire protection and detection system used within the operating area, all personnel shall attend semiannual refresher training sessions designed to update their knowledge of the equipment and procedures to be used in the event of a fire.

b. Local fire department officers and firefighters shall be invited to periodic orientation tours of the facilities to aid them in their preplanning or familiarization of the location of the equipment.

c. Personnel of organization support activities, such as supply, transportation, procurement, contract negotiation, and building maintenance activities, who are included in the Contingency Plan should be periodically involved in mock disaster exercises so they will know the role they have to play in the organizational plan.

385. GENERAL REPORTING.

a. It is vital to include reporting as an integral part of this standard practice. The results of the reporting procedures are to, (a) spread the knowledge and experience gained by one agency to the rest of the Federal family, (b) to provide a data base to evaluate the results of the criteria contained herein, and (c) to serve as an indicator and justify the need for changes.

b. Investigation of all significant fires involving essential computer operations is needed to determine what happened and to prepare the necessary reports. There are many "experts" in the Federal family whose services may be secured to assist in preparing a well-balanced, total system review of an incident, e.g., fire protection, operations, electrical, mechanical safety, etc., engineers and specialists. Aid and assistance should be sought from these "experts" in other Federal agencies to broaden the experience upon which an investigation will be based.

386. REPORTING INCIDENTS/MISHAPS. All incidents or mishaps shall be reported in accordance with FAA Order 3900.19B, FAA Occupational Safety and Health Handbook.

SECTION 5. MISCELLANEOUS

387. DESTRUCTION OF COMPUTER-GENERATED OUTPUT. Special destruction procedures are not required for the great majority of computer generated reports and listings. This generalization applies as well to waste paper products generated within computer equipment rooms as a result of such errors as printer misalignment, etc. However, those paper products which do not contain sensitive information, as defined by FAA Order 1370.47A, and/or other information which should not be given general circulation, shall be rendered unintelligible by shredding, cutting, pulverizing, or other means approved by the cognizant security division. Destruction of sensitive waste material, not released to a user office, shall be the responsibility of the AISSO; otherwise, destruction will be accomplished by the using component. Cognizant national offices and services may further amplify this paragraph by specifying what computer processed reports or forms must be destroyed by special security techniques.

388. PROTECTION OF BACKUP SOFTWARE AND VITAL RECORDS. AISSM's, either as part of a comprehensive contingency plan or as a separate action, shall determine those files and programs (to include the operating system) which are essential to organizational operation or are most subject to fraud and provide suitable, secure offsite storage to assure the availability of accurate copies of these files and programs. This will provide indepth protection against natural or malicious incidents, as well as facilitating recovery operations.

389. SECURE STORAGE OF SENSITIVE OR CONTROLLED FILES AND PROGRAMS. Sensitive information, programs, or documentation files having a high potential for fraudulent manipulation shall be secured after normal duty hours to prevent unauthorized access.

390. - 399. RESERVED.

FIGURE 3-1

FIRE HAZARD CLASSIFICATION OF EXPOSURE OCCUPANCIES

A. LIGHT HAZARD OCCUPANCIES. Those with less than 10 pounds of ordinary combustibles per square foot of gross floor areas and having a fire potential of less than 1 hour, for example;

Classrooms, conference rooms, auditoriums, dining rooms Courtrooms,
detention cells, fire rooms using metal file cabinets
Hospital areas, libraries, excluding large stack areas
Offices using wooden furnishings, less than one person per 20 square
feet of floor area
Rest rooms and locker rooms (with metal lockers)
Offices using metal furniture

B. MODERATE HAZARD OCCUPANCIES. Those with 10 to 20 pounds of ordinary combustibles per square foot of gross floor area and having a fire potential of 1 to 2 hours, for example;

Drafting rooms, mapmaking rooms
Electronic, electrical, and similar laboratories not using flammable liquid
Mail rooms, post office workrooms
Offices using wooden furnishings where personnel occupancy exceeds one person per 200 square feet
Parking garages, printing and reproduction operations
Shops not involving flammable liquids or production woodworking

C. HIGH HAZARD OCCUPANCIES. Those with more than 20 pounds of ordinary combustibles per square foot of gross floor area or involving significant amount of flammable liquids; having a fire potential in excess of 2 hours; or with a potential of fast fire spread which may endanger life and/or the structure, for example;

Automobile servicing, fueling, or repairing
Chemical or other laboratories involving significant amounts of flammable liquids
Flammable liquid operations
General storage warehouses, trash rooms
Library stacks and open shelf file rooms
Major machine shops using large amounts of combustible cutting oils or machining of pyrophoric metals
Paint shops, production woodworking shops

NOTE 1: Ordinary combustibles are defined as materials such as paper and wood having an average British Thermal Unit (BTU) potential heat release of about 8,000 BTU's per pound.

NOTE 2: The above examples are based on typical operations and average distribution of combustibles. Judgement must be used and the level of occupancy hazard increased or decreased where the conditions are not typical, and the combustibles involved present either more or less fine potential than the typical situation. For example, mail rooms with low activity or drafting rooms using modern metal furniture are usually light rather than moderate hazards. Conversely, if an office equipped with metal furniture habitually contains very large quantities of paper and similar combustibles, which are not contained within file cabinets or other metal containers, that office would be a moderate rather than a light hazard.

CHAPTER 4. COMPUTER NETWORK AND REMOTE ACCESS SECURITY CONSIDERATIONS

400. GENERAL. The joining of computer and communications technologies represents a major advancement in computer science. While this development has contributed significantly to the diversity and geographical flexibility which characterize modern large-scale computer systems, certain risks pertaining to system integrity, confidentiality of data, and denial of system use are also introduced. Communications-related security vulnerabilities include:

a. The potential for unauthorized access to sensitive and unclassified National security information increases with the amount of remotely accessible data available, the number of individuals afforded access to remote access equipments, and the geographical distribution of the network.

b. The hazard of the interception of data communications is always present. The ability to intercept also permits the ability to modify and alter data or to extract information from the system. Computer codes and formats, though not readily legible, afford no true communications security.

c. The accidental or intentional modification of addresses may result in the transmission of data to the wrong terminal device; thereby permitting unauthorized access to the information.

401. SCOPE. The following paragraphs of this chapter apply to all FAA AIS, telecommunications systems and networks. COMSEC concerns should be considered in the design and planning for all future FAA systems. Commercial time-sharing remote access security considerations are set forth in paragraph 408.

402. TRANSMISSION OF CLASSIFIED INFORMATION. As specified by Order 1600.8B, Communications Security (COMSEC), classified information shall not be introduced into a remotely accessed FAA computer system while operated in a teleprocessing environment, unless the communication links between remote terminals and/or computer processors have been secured with National Security Agency (NSA) approved cryptographic equipment. Also, all networks that will transmit classified information shall be evaluated in accordance with National Computer Security Center Report, "Department of Defense Trusted Network Evaluation Criteria" and other NSA documents as required. The evaluation shall be approved in writing by the Office of Civil Aviation Security prior to any transmission actions.

403. TELEPROCESSING OF SENSITIVE OR UNCLASSIFIED NATIONAL SECURITY INFORMATION. The increasing concern for the confidentiality, integrity, and security of data resident on remotely accessed computer systems requires that possible COMSEC vulnerabilities be considered before sensitive or controlled data are introduced into an existing system or during the analysis and design process leading to the creation of a new system.

a. Data Encryption Standard. NBS FIPS PUB 46, Data Encryption Standard (DES), sets forth a standard that will be used by Federal departments and agencies for the cryptographic protection of computer data when the following conditions apply:

(1) An authorized official or manager responsible for data security or the security of any computer system decides that cryptographic protection is required; and

(2) The data are not classified according to the National Security Act of 1947, as amended, or the Atomic Energy Act of 1954, as amended.

However, Federal agencies or departments which use cryptographic devices for protecting data classified according to either of these acts can use those devices for protecting unclassified data in lieu of the standard. In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.

b. Sensitive Information Analysis. An analysis shall be performed under the direction of a responsible authority to determine what information is sensitive, unclassified National Security information or otherwise of high value. In addition, a risk analysis should be conducted in accordance with chapter 11 of this order to determine risk of exploitation and vulnerabilities to unauthorized disclosure or undetected modification during transmission. Data that is considered sensitve, or unclassified National Security information should be cryptographically protected during transmission outside the controlled area of the DPA's involved. Other data that is considered to have a high value should also be cryptographically protected if the risk analysis indicates there is sufficient threat to warrant such measures. The costs of providing cryptographic protection using this standard as well as alternative methods of providing this protection and their respective costs should be projected. A responsible authority then should make a decision, based on these analyses, whether or not to use cryptographic protection and this standard.

c. Use of Data Encryption Within FAA. Prior approval for the use of data encryption techniques shall be obtained from the Designated Approving Authority (DAA), to ensure appropriate protection is provided for the AIS or network involved.

404. OTHER TECHNIQUES FOR ENHANCING SYSTEM INTEGRITY AND ACCESS CONTROLS. Certain hardware and software measures can be incorporated or designed into computer networks which will enhance the level of system security against communication-related threats. System designers or program managers should be alert to the possibilities of incorporating one or a combination of the following techniques were derived from NBS FIPS PUB 83, Guidelines On User Authentication Techniques For Computer Network Access Control.

a. Accuracy Controls. Such internal system accuracy controls as parity checks, character redundancy codes, memory bounds checks, or any other similar error detection techniques can be used to assure security, as well as provide error-free data transfers.

b. Terminal Identification. This involves the use of hardware or software techniques that provide unique and positive identification of the terminal device.

c. Improved Terminal User Identification. Equipment is now available that will provide a greater degree of user identification than the password systems now commonly used. These measures include the use of magnetically coded badges and hand geometry.

405. DISABLING OF REMOTE TERMINALS. FAA remotely accessed, general purpose computer systems shall be provided with the capability of disabling or disconnecting, either physically or by software, any or all of the remote terminals attached to the system. This disconnect capability will be utilized during periods of dedicated processing or when the area housing the terminal is unoccupied and cannot be physically secured to prevent possible unauthorized use of the terminal after normal duty hours.

406. USER IDENTIFICATION AND AUTHENTICATION. FAA AIS and networks shall have and use a software user identification and authorization capability. The use of passwords is the most widely used authentication technique employed to grant system access. This function or an equivalent user identification and authorization feature will be implemented and strictly adhered to. Passwords can also be employed to relate system users with specific system resources, particular applications, data files, or system functions. Additional information on this subject may be found in FIPS PUB 112, Standard for Password Usage. This document shall be used to determine the composition, length range, source, ownership storage, etc., of the password. The following guidelines shall be followed in the implementation of a password protection mechanism:

a. Passwords shall be managed by the AISSO for AIS access.

b. Passwords shall be managed by the NSO for network access.

c. Passwords shall be attributable to individuals in order to place individual responsibility and reduce the unauthorized use of the system.

d. Passwords (alpha - numeric characters) shall not be based upon information that can be derived by the knowledge of the authorized user's birthdate, initials, home address, etc. Passwords should be randomly generated, either manually by the AISSO/NSO, or by a software (program or operating system) random generator, at a length of 4-8 characters.

e. Passwords shall be changed at given intervals, but at least every 90 days or whenever a compromise is known or suspected.

f. Passwords shall not be shared or disclosed to other users.

g. Responsible managers shall assure that system or network authenticators held by users that resign, retire, or who no longer require access are removed from system access tables promptly upon the receipt of notification of such a change in a user's status.

407. PROTECTION OF AUTHENTICATORS. System administrators, regional or center Consolidated Personal Management Information System (CPMIS) managers, and individual terminal users shall assure that unique authenticators will be protected to prevent compromise. Such authenticators include user and file passwords or lockwords; master system access directories, and access codes to commercial time-sharing systems. Additional information is contained in NBS FIBS PUB 83 and should be utilized as required. Protection of these authenticators will include the following considerations:

a. Software Protection. Lookup tables, routing tables, user profile directories, or other files associated with controlling security access or services shall not be accessible to user application processes, or system resources operated under user control. Seperate control systems, unique to the management of security services shall be provided to designated personnel for the implementation of the security management function.

b. Security of Master Hardcopy Authentication Files or Listings. Hardcopy listings or other paper materials, to include master copies of user identifiers and individual passwords that afford access to an FAA AIS, network, or commercial time-sharing system used by FAA, shall be maintained in the strict custody of the system or facility manager or his designated representative. As a minimum, these files shall be stored in a metal file container equipped with a lock bar and secured with a three position, changeable GSA-approved combination padlock or key-operated padlock that is incorporated into the FAA locking system, as prescribed in Order 1600.6B.

c. Protection of System Authenticators. Individuals shall be responsible for protecting unique, personal system authenticators which allow them to use or access a system. Protection afforded these authenticators shall be sufficient to ensure that they are not compromised through carelessness or negligence.

408. COMMERCIAL TIME-SHARING SERVICE-MANAGERIAL SECURITY RESPONSIBILITIES. FAA employees who are responsible for managing or administratively controlling the use of commercial time-sharing services by FAA employees or contractors have a central role in assuring that these systems are used in a manner that is clearly consistent with the best interest of the FAA. The requirements set forth in PBS FIPS PUB 83 and 112 are applicable to all commercial time-sharing services. Included in the security responsibilities inherent in the management of system utilization are the following:

a. Prevention of Misuse. Any indication of the unauthorized use of diversion of a commercial time-sharing service system resource which results in the FAA being billed shall be reported promptly to the appropriate level of management, who will promptly notify the servicing security element.

b. Maintenance of User Authorization Lists. Procedures shall be established to assure that those individuals afforded access to commercial time-sharing service systems have a valid, continuing requirement to use these services. Individuals who no longer require access shall be promptly removed from all access tables.

409. COMMERCIAL TIME-SHARING SYSTEM-USER SECURITY RESPONSIBILITIES. Authorized users of the various commercial time-sharing services to which FAA subscribes shall utilize the following procedures to assure the integrity of data resident on files, and to prevent misuse of terminals by unauthorized users:

a. Authenticator Protection. Users shall utilize the overstrike or character suppression capability designed into most time-sharing systems. If these cannot be utilized, users shall assure that passwords or other terminal access data are not left on discarded printouts, discarded listings, or unattended video display terminals.

b. Terminal Security. Upon completion of input/output operations, when unable to monitor the use of live terminals, users shall initiate log-off procedures, secure the terminal room, and/or take other precautions so as to assure that live terminals are not available for unsanctioned use as required by paragraph 319. Sensitive or proprietary information contained on listings or printouts should not be discarded indiscriminately but destroyed as appropriate by the terminal user in accordance with Order 1600.15D.

410.-499. RESERVED.

CHAPTER 5. COMPUTER PROCESSING OF CLASSIFIED INFORMATION

500. GENERAL. The computer processing of classified national security information, as defined by E.O. 12356, National Security Information, is a unique operational situation which requires the adoption of more restrictive security measures than those used during routine data processing activities.

a. NSDD-145, National Policy on Telecommunication and Automated Information System Security, requires an evaluation of all Automated Information Systems in accordance with Department of Defense 5200.28-STD Department of Defense (DOD) trusted computer system evaluation criteria (the orange book).

b. The objective of this increased level of security is to preclude the deliberate or inadvertent access to classified information by unauthorized persons during or after the computer processing of classified information by FAA-owned or leased computer systems.

501. SCOPE. The provisions of this chapter apply to all FAA-owned or leased computer systems when these are used to process, store, or produce classified material. It also covers computers systems operated by FAA contractors or computer service organizations.

502. AUTHORITY TO USE FAA COMPUTERS TO PROCESS CLASSIFIED INFORMATION. Facility or program managers who desire to use FAA AIS equipment to process classified information for either FAA or on behalf of another Federal agency shall request for prior accreditation approval from the DAA.

a. The request is to be submitted in the form of an accreditation document to the AISSC for review and recommendation. The accreditation request is to be in compliance with chapter 15 of this order. An accreditation request shall be made for each classified application processed. This document shall prescribe the application, the classification of data, anticipated frequency of processing, and the applicable security measures to be taken at the facility in sufficient detail to permit a determination to be made as to their adequacy.

b. The Office of Civil Aviation Security shall evaluate the request in accordance with the DOD 5200.28-STD, NACSI 5004 National COMSEC Instruction, TEMPEST Countermeasures for Facilities within the United States, and other National Security Agency documents as required. If the evaluation is positive, then ACS-1 will grant approval in writing.

503. PERSONNEL SECURITY CLEARANCES. When classified information is processed in an FAA computer facility, access to the information shall be limited to those personnel who are essential to the processing of this data. This includes management, data preparation, machine operations, output distribution, and where applicable, program development, testing, and equipment maintenance. These personnel shall be cleared prior to the start of the processing to a level commensurate with the highest classification and most restrictive category of the information involved.

504. ADDITIONAL SECURITY MEASURES TO BE IMPLEMENTED DURING CLASSIFIED PROCESSING. The following additional security measures shall be implemented to provide adequate protection to this material:

a. Dedicated Mode of Operation. The ADP system and the computer housing the system shall be operated in a dedicated mode (system high).

b. Increased Personnel Access Controls. Additional physical and procedural controls shall be imposed to ensure that only authorized personnel having the appropriate clearance and managerial authorization are permitted to enter the central computer facility during periods of classified processing. The computer equipment room shall be designed as a "closed area," in accordance with the provisions of Order 1600.2C, while classified processing is being accomplished.

c. Disabling of Remote Input/Output Equipment. All remote input/output devices shall be electronically and/or physically disconnected from the computer system and the telecommunications program disabled. Disconnection will be accomplished at a point within the central computer complex.

505. RETURN TO NORMAL OPERATING CONDITIONS. Following the conclusion of classified processing and before the computer facility can return to its normal operating environment, certain procedures must be completed to sanitize electronically the equipment and to secure physically the classified information used and/or processed in the central computer facility. All procedures shall be in accordance with the National Computer Security Center Guideline CSC-STD-005-85, Department of Defense Magnetic Remanence Security. These procedures shall include:

a. Inspection of data processing equipment and operator console ribbons to assure that classified information cannot be retrieved from the source. If new ribbons have been installed prior to the period of classified processing, these must be removed and securely stored or destroyed.

b. Sanitization of internal memory by overwriting.

c. Sanitization of discs used as temporary work space by overwriting.

d. Sanitization of scratch tapes by overwriting or by using an approved magnetic degausser.

e. Securing of all classified computer storage media and other material that will remain in the ADP facility in accordance with the requirements of chapter 6 in Order 1600.2C.

506. MARKING OF CLASSIFIED OUTPUT AND STORAGE MEDIA. Hard-copy output shall be marked with the appropriate national security classification, as required by FAA Order 1600.2C. These markings will be placed on the front cover, first page of text, and last page of text and back cover. This material will then be handled in accordance with the provisions of FAA Order 1600.2C. It is not necessary to

mark each card deck or each card comprising a deck, but the overall classification should be indicated in a distinctive manner on the cards or holder. The classification of magnetic tape reels and disc packs will be indicated by affixing adhesive labels to the tape reels, disc packs, and their container, or by the use of color-coded containers. Classified hard copy, tape reels, and card decks will be incorporated into the appropriate classified information security control point servicing the AIS facility.

507. COMSEC. All requirements for communication security and the use of cryptographic systems within FAA are defined in Order 1600.8C, Communication Security.

508. MAINTENANCE OF DOCUMENTATION. Facility managers shall maintain complete and accurate documentation for all application programs used to process classified information.

509. CLASSIFIED VERSION OF OPERATING SYSTEM. Those installations which frequently perform classified processing should maintain a duplicate version of the operating system or supervisor program to be used only during periods of dedicated operation. This shall be secured in a container approved for storage of classified information.

510. INTERPRETATION AND GUIDANCE. Questions on interpretation of the provisions of this chapter on their application to specific problems shall be referred to the appropriate FAA regional/center headquarters security element or to the National AIS Security Program Manager.

511.-599. RESERVED.

CHAPTER 6. DATA SECURITY CONTROLS FOR SENSITIVE INFORMATION SYSTEMS

600. GENERAL. This chapter addresses data security controls for sensitive batch jobs and teleprocessing system jobs.

601. SCOPE. This chapter is directed to general purpose data processing operations (DPO) and teleprocessing systems that support FAA administrative requirements.

602. CONTROL OF SENSITIVE BATCH JOBS. Adequate security demands positive control of automated and manual processing within the system and facility. Controls must be detailed, especially between functions, for review and audit. The following guidance is for sensitive operations:

a. Job Control Documents. Prior to acceptance, each request for service or job submitted should be verified through job identification numbers, passwords, and/or signatures. Once accepted, the job should be controlled by a single document. This document should contain the identification of the submitter, processing to be performed, control or transaction totals, classification and sensitivity level, program and file requirements, run time, output verification instructions, and distribution. All procedural requirements should be identified and verified at major functional transfer points (such as, upon receipt and logging, when scheduled for production, when programs and files are identified and withdrawn from the library, and when passed to operations).

b. Input/Output Control. All material entering and leaving the facility (such as, hard copy printouts, magnetic tape reels, disks or card decks) must pass through a control element for review. Personnel assigned to this element must be cleared for the highest classification of data handled. Functions performed during input/output control should include:

(1) Receipting for input.

(2) Preparing the master control document.

(3) Recording of document counts and control totals.

(4) Initiation of corrective action on improper inputs.

(5) Submitting source documents to data preparation.

(6) Verifying clearances of personnel receiving output.

(7) Checking results of data validation runs.

(8) Identifying library requirements (such as, tapes or disks)

(9) Submitting jobs for processing.

(10) Ensuring that output is receipted for.

(11) Reviewing process accounting data to verify counts, hash totals, and whether the processing time is reasonable.

(12) Reviewing output for processing errors, proper security markings and caution statements, if required.

(13) Approving release of materials.

c. Scheduling and Job Control. Well-defined procedures for scheduling, processing, and verifying job control instructions are essential to the security of sensitive operations.

(1) Scheduling. Job scheduling activities, either manual or automated, define the data, programs, and system components which will interact during processing. Effective procedures should identify job classes by security classification, in addition to the various types of resources required.

(2) Job control. To ensure adequate control, job execution instructions should be well detailed (for example, run time, dependent jobs, core requirements, input/output devices). Job controls or command language capabilities and instructions must be complete and fully utilized to minimize manual intervention. Job stream controls are useful in enforcing user identifications; specifying task, storage, and device requirements; and stating required responses to exceptional circumstances (such as, execution abort, device malfunction, and data errors). All job control instructions and instruction decks must be safeguarded and job streams validated prior to being passed to operations for execution.

d. Logs. System facilities for maintaining journals and operating logs must detail systems activities, including all runs, errors, restarts, interrupts, control instructions, and operator interventions. Copies will be retained for at least 60 days. Operator console records must be reviewed daily or at the end of each shift for effectiveness of security controls. This review will be conducted by the AISSO or by supervisory personnel under the direction of the AISSO.

603. CONTROL OF TELEPROCESSING SYSTEMS JOBS. The increased operational flexibility of teleprocessing systems and their remote nature increases their vulnerabilities and the opportunity for exploitation. Therefore, DPA/AIS management must ensure that a complete security program supports the operation prior to commitment to a teleprocessing system. This security program must provide a degree of control which is positive, detailed, and ensures that only authorized users enter the system, manipulate data, and receive output.

a. Control Documents. Although the system of control documents in a teleprocessing system is different from those in a batch oriented system, use of the teleprocessing system must be controlled and capable of being audited. The audit trails of a teleprocessing system must be capable of identifying all users and time of access. The audit trails must also be capable of journaling the files and applications used by the individual accessing the system and the purpose and activity performed during the access. These requirements are mandatory for all new FAA systems.

b. Input and Output Controls. Input and output controls.

(1) Input will be controlled by ensuring that all persons accessing a teleprocessing system are authorized users and that they are authorized to process the data (for example, read, write, update, and so forth). The system will allow the user the minimum resources necessary to accomplish the task. Authorized users must be provided access and privileges as general users of the system and "locked out" of all specific, sensitive files and processes unless approved by the DPA/ATS management and/or AISSO. This approach supports the need-to-know principle.

(2) Output must be linked to the authorized recipient of the material. If the output is in the form of hard copy printouts, cards, or magnetic media at a device local to the host computer, it must be identifiable and controlled as if generated in a batch environment. The system must have the capability to determine if the reouestor or an authorized representative is present prior to initiating generation of output at that remote device (that is, printouts must not be generated at unattended printers). Output at remote devices will be receipted in an output control log.

c. Scheduling. Scheduling must be controlled to ensure that an authorized user does not inadvertently or intentionally seize control of more resources than desired by system managers. The automated scheduler must order jobs by priority so that a denial of service situation does not develop.

d. Logs. A system of automated logs must journal all system activity as stipulated in paragraph 602d.

604. - 699. RESERVED.

CHAPTER 7. ADMINISTRATIVE SECURITY CONTROLS

700. GENERAL. Procedural security measures can be cost-effective since they usually involve a minimum of financial expenditures while producing a higher level of security. This chapter addresses the internal procedures that must be implemented to provide that appropriate security protection.

701. SCOPE. This chapter is applicable to all DPA's operating general purpose and special purpose computer systems.

702. STANDARD OPERATING PROCEDURE. A standard operating procedure will be maintained by all DPA/DPI outlining the AIS security requirements for each facility.

703. MANAGEMENT SECURITY CONSIDERATIONS. The effectiveness of DPI's physical and administrative security measures is in large part dependent upon the reliability and trustworthiness of the staff. Personnel-related considerations include the selection of suitable individuals to fill AIS positions, assuring employee awareness of their security obligations, monitoring their compliance with security requirements, tailoring assigned responsibilities to minimize opportunities to circumvent security safeguards, and maintaining positive security controls which assure an efficient and secure data processing environment.

a. Separation of duties. It is mandatory that key duties within a facility be separated so as to preclude any one individual from adversely affecting the system. Procedural checks and balances should be built into manual processes and interfaces so that deviations from the separation of duties principle can be detected and reported to the AISSO. In the operations areas, the "no alone" rule (no individual will be in the area alone; a second person must be present) should be followed for personnel safety reasons and to deter willful or unknowing security violations. Inability to have two people present should be included in the risk assessment.

b. Delineation of responsibilities. Duties, responsibilities, privileges, and specific limitations of all personnel involved in the operation of a facility bearing a sensitivity designation must be specified in writing and periodically reviewed by management or security personnel.

c. Security indoctrination and training. One of the most effective features of a security program is the training and indoctrination conducted to inform personnel of their security responsibilities, system threats, vulnerabilities, and effective countermeasures. Automation security training must be presented on assumption of duties, refreshed annually, and tailored to individual responsibilities within the DPA/DPI.

d. "Closed-shop" operations. All applications software development, maintenance and modification activities, machine-room operations, system programming, data preparation and editing, and library operations of the DPA/DPI must be conducted under closed-shop conditions. Such operations, and the resulting documentation, must be positively controlled. Access will be allowed selectively to DPA/DPI personnel only on the basis of established need.

e. Protection of documentation. The safeguarding of all documentation supporting applications and systems programs and their interaction is vital to effective security. Protection must be extended to all documentation revealing the logic, methodology, or procedural aspects of system operations. This includes, but is not limited to:

(1) Software development documents (such as, system and logic diagrams, decision tables, listing of program code, test data, data editing, error detection, test, and verification coding).

(2) Debug routines and output (such as, core dumps, memory snapshots, trace routines).

(3) Master control software for loading and executing programs.

(4) Operating instructions (such as, run books and operator's manuals).

(5) Documentation pertaining to software, systems errors, or flaws (such as, security violation reports, generic system flaws, justifications for software or modification, or other software maintenance requirements).

f. DPA Security Profile. A formal DPA Security Profile will be developed by the AISSO and approved by the AISSM for each AIS. The purpose will be to describe or diagram the physical facilities, equipment locations and relationships, and other operating characteristics (for example, types and amounts of sensitive processing) of the DPA/DPI. This profile will include architectural drawings or diagrams of physical facilities, computer center floor plans, equipment inventories, equipment interface diagrams, communications schematics (including connections to external communications links or networks), and wiring diagrams. The profile shall be maintained and safeguarded by the AISSO. Changes to the physical, electronic, or electrical configuration must be coordinated with the AISSO. When changes occur, these must be included in a revised profile which will be issued simultaneously with the physical changes. In addition, these changes should be noted for consideration in the risk assessment. Appendix 3, Short Form Risk Analysis, may be used as the a profile for Office Automation (OA) systems.

g. Organizational placement of the AISSO. As the key individual responsible to the DPA/DPI manager for conducting an effective security program, the AISSO must report directly to that authority on security-related matters. While this responsibility implies full-time security duties, austere manning may make this impossible or impractical. Therefore, depending upon sensitivity level designation, AISSO responsibilities can be fulfilled on a part-time basis. The AISSO should not report to any individual who is responsible for production or operations, with regard to AIS security, and should not have a vested interest in keeping the system operational after a possible security problem has been discovered. This is to ensure a sense of objectivity concerning decisions which may affect operational requirements and to avoid a conflict of interest.

704. ADMINISTRATıVE ACCESS CONTROLS. Appropriate security controls will be implemented during operational hours to assure that only authorized persons are permitted to enter the computer room and supporting offices. All computer rooms and support facilities will be secured upon completion of the duty day or at anytime the facility is unoccupied (such as during a fire drill, bomb threat, and so forth).

705. PROGRAM CHANGES. Procedures shall be implemented so that a formalized approval and/or authorization mechanism is established over modifications made to sensitive programs or those having high potential for fraudulent manipulation. It is also important that a record of these changes be made and that a copy of the modification be filed with the program run manual. It is recognized that this provision is more applicable to general purpose, applications-oriented data processing activities, but the use of this procedure should be considered for relevant national or local special purpose computer programs.

706. MAINTENANCE OF DOCUMENTATION. The preparation and maintenance of program documentation, prepared in accordance with FAA Order 1370.53, Uniform Documentation Standards for the Development, Maintenance, and Operation of Automated Data Systems, is important as a security measure, as well as an operational necessity. AIS managers should require, particularly with respect to programs used to process sensitive or controlled data, the secure maintenance of documents and records which fully and accurately describe the system and changes made to it.

707. AIS MEDIA CONTROL AND PROTECTION. Administrative procedures should be utilized to supplement the physical protection afforded AIS storage media. Some of the potential hazards which can be covered by administrative safeguards include the following:

a. Labeling. Containers, tape reels, disc packs, and card decks should be clearly identified as to their contents to prevent accidental release.

b. Prevention of Inadvertent Destruction. Various safeguards can be used to prevent accidental writing on magnetic tape containing master files or programs. These can include the presence or absence of a removable ring. The absence of the ring will inhibit writing on the tape. Specific operational instructions should also be established to cover such incidents as dropped disc packs, etc.

c. Media Library Controls. AIS media library procedures should be developed for systematic storing of media and controlling of the media under library control.

Library controlled AIS storage media shall not be stored outside of the central media library. Exceptions are permitted for: (1) temporary operational storage within the computer equipment room, and (2) remote storage of vital data security and backup purposes, as prescribed in Order 1350.14A, Records Management.

d. Control of Access to Data Storage Areas. Besides the physical security measures established for data storage areas, appropriate managerial controls must be implemented to reinforce these physical safeguards.

e. Magnetic Media Security. Appropriate measures shall be implemented to prevent unauthorized individuals from obtaining sensitive data from internal memory work areas, scratch discs, scratch tapes, floppy disks, etc. It is important that all computer users be aware of the retentive properties of magnetic storage media and be aware of the known risks in erasing and/or releasing magnetic storage media. They must use approved security procedures that will help prevent disclosure of classified or sensitive information. Administrative procedures shall be implemented based on the National Computer Security Center Report CSC-STD-005-85 "Department of Defense Magnetic Remanence Security Guideline" dated 15 November 1985.

708. IDENTIFICATION OF CLASSIFIED OR SENSITIVE INFORMATION SUBMITTED FOR COMPUTER PROCESSING. It shall be the responsibility of the organizational component requiring data processing support to assure that the AIS system or facility manager is advised of any requirement to provide security for sensitive or classified material submitted for computer processing that exceeds the protective measures outlined in chapters 5 and 6.

709. MISUSE OF FUNCTION AND PRIVILEGES. Much of the recent design and development efforts have been directed toward simplifying system usage as well as enhancing the variety of system resources available to the user. However, these developments, together with the ever increasing concentration of high-risk data resident on computer systems, also result in greater opportunities for system abuse. FAA employees or other individuals authorized access to an FAA computer system who knowingly misuse or abuse a system will be subject to disciplinary actions under the provisions of Order 3750.4, Conduct and Discipline Handbook, as well as any criminal penalties which may result from data alteration, system misuse, or diversion of system resources for personal gain or profit.

710. INADVERTENT RECEIPT OF DATA. Data generated by or intended for input into a general purpose computer system may be misrouted or mishandled, thus resulting in the inadvertent receipt of possibly sensitive data by someone who would not normally have access to it. This can occur as the result of a malfunction of system hardware or software, the misrouting of data through communication lines, or human errors in distributing input or output. Individuals inadvertently receiving such data shall promptly report this fact to the appropriate system administrator or AIS facility manager. AIS system or facility managers shall maintain a log of these events for subsequent diagnostic analysis by appropriate systems and/or security personnel. Hard-copy output which contains either sensitive or controlled information, as defined by Order 1370.47A, and all input documents will be returned to the appropriate system manager or AIS facility manager. Corrective measures shall be initiated to eliminate the causes of repeated loss of input or output materials.

711. REPORTING LOSS, THEFT, OR DAMAGE. Incidents of loss, theft, or damage to computer equipment, software, and data shall be reported immediately to the appropriate security element by the facility manager and/or other responsible personnel. Reporting requirements shall be communicated to FAA personnel who are engaged in the operation, programming, and administration of FAA computer systems, related facilities, and related activities, to include commercial time-sharing.

a. Suspected or Alleged Fraud or Theft. Incidents of systems misuse or abuse, or other use of AIS systems contrary to law or FAA regulations, shall be reported to the security office servicing the AIS facility for arranging for investigation when appropriate.

b. Property Damage or Destruction. Incidents of malicious damage or theft of AIS equipment or records shall be reported, as appropri_te, to the cognizant security element fo: investigation and, if appropriate, to the Federal Bureau of Investigation (FBI). In emergency situations where time is of the essence, notification may be made to the FBI, to the building protective services office, or to the law enforcement office with jurisdiction over the location, with immediate notification also to the cognizant security element.

c. Property Record Reconciliation. Incidents of lost, damaged, or destroyed computer equipment or software should be reported on FAA Form 4630-8, Report of Survey, in compliance with Order 4630.3B, Survey of Lost, Damaged, or Destroyed Government Personal Property. Incidents related to thefts and losses of government and personal property, at Washington headquarters shall be reported in accordance with Order WA 1600.2C.

712. SECURITY INCIDENTS. All security incidents will be reported to the respective AISSO. The AISSO will conduct a preliminary inquiry to determine if an actual violation occurred. The matter then will be reported to the servicing Civil Aviation Security Division's AISSM. If warranted, an investigation will be initiated. The manager of the security element shall review all security incident reports and advise the region/center director as to whether a system has been penetrated, compromised, misused or a security violation has occurred. Any suspected or confirmed violation or compromise of classified information will be investigated in accordance with Order 1600.2C. Other suspected or confirmed incidents will be reported to ACS-1 with findings and corrective action taken to preclude reoccurrence.

713.-799. RESERVED.

CHAPTER 8. HARDWARE/SOFTWARE SECURITY

800. GENERAL. The National Security Agency/National Computer Security Center has established a methodology for evaluating the security of computer systems. The information in this chapter is based on the Department of Defense trusted computer system evaluation criteria, DOD 5200.28-STD. It is the intent of this chapter to provide only general guidance and that a detail evaluation of all computer systems will be in accordance with DOD 5200.28-STD (called the orange book).

a. The trusted computer system evaluation criteria defined in the orange book and in this chapter, apply primarily to trusted, commercially available AIS. They are also applicable, as amplified below, to the evaluation of existing systems and to the specification of security requirements for AIS acquisition. Included are two distinct sets of requirements: 1) specific feature requirements; and 2) assurance requirements. The specific feature requirements encompass the capabilities typically found in information processing systems employing general-purpose operating systems that are distinct from the applications programs being supported. However, specific security feature requirements may also apply to specific systems with their own functional requirements, application or special environments (e.g., communications processors, process control computers, and embedded systems in general). The assurance requirements, on the other hand, apply to systems that cover the full range of computing environments from dedicated controllers to full range, multilevel secure resource sharing systems.

b. Designers of new automated ATC-related systems shall consider requirements for incorporating hardware/software security controls into equipment and software specifications for ATC and related systems.

801. SCOPE. The criteria set forth here has been developed to serve a number of intended purposes:

a. To provide a standard to manufacturers as to what security features to build into their new and planned commercial products in order to provide widely available systems that satisfy trust requirements (with particular emphasis on preventing the disclosure of data) for sensitive applications.

b. To provide the U.S. Government with a gauge with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.

c. To provide a basis for specifying security requirements in acquisition specifications.

802. TRUSTED COMPUTER SYSTEM EVALUATIONS. Evaluations can be delineated into two types: (1) an evaluation can be performed on a computer product from a perspective that excludes the application environment; or (2) it can be done to assess whether appropriate security measures have been taken to permit the system to be used operationally in a specific environment. The former type of evaluation is done by the National Computer Security Center through the commercial product evaluation process.

a. The latter type of evaluation, i.e., those done for the purpose of assessing a system's security attributes with respect to a specific operational mission, is known as a certification evaluation. It must be understood that the completion of a formal product evaluation does not constitute certification or accreditation for the system to be used in any specific application environment. On the contrary, the evaluation report only provides a trusted computer system's evaluation rating along with supporting data describing the product system's strengths and weaknesses from a computer security point of view. The system security certification procedure, done in accordance with the applicable policies of the issuing agencies, must still be followed before a system can be approved for use in processing or handling classified or sensitive information. Designated Approving Authorities (DAA) remain ultimately responsible for specifying the security of the systems they accredit.

b. The trusted computer system evaluation criteria will be used directly and indirectly in the certification process. Along with applicable policy, it will be used directly as technical guidance for evaluation of the total system and for specifying system security and certification requirements for new acquisitions. Where a system being certified employs a product that has undergone a commercial product evaluation, reports from that process will be used as input to the certification evaluation. Technical data will be furnished to designers, evaluators and the designated approving authorities to support their needs for making decisions.

803. FUNDAMENTAL COMPUTER SECURITY REQUIREMENTS. Any discussion of computer security necessarily starts from a statement of requirements, i.e., what it really means to call a computer system "secure." In general, secure systems will control, through use of specific security features, access to information such that only properly authorized individuals or processes operating on their behalf will have access to read, write, create, or delete information. Six fundamental requirements are derived from this basic statement of objective: four deal with what needs to be provided to control access to information; and two deal with how one can obtain credible assurances that this is accomplished in a trusted computer system.

a. Requirement 1 - SECURITY POLICY - There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object. AIS of interest must enforce a mandatory security policy that can effectively implement access rules for handling sensitive (e.g., classified) information. These rules include requirements such as: Individuals lacking proper personnel security clearance shall not obtain access to classified information. In addition, discretionary security controls are required to ensure that only selected users or groups of users may obtain access to data (e.g., based on a need-to-know).

b. Requirement 2 - MARKING - Access control labels must be associated with objects. In order to control access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object wich a label that reliably identifies the object's sensitivity level (e.g., classification), and/or the modes of access accorded those subjects who may potentially access the object.

c. Requirement 3 - IDENTIFICATION - Individual subjects must be identified. Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with. This identification and authorization information must be securely maintained by the computer system and be associated with every active element that performs some security-relevant action in the system.

d. Requirement 4 - ACCOUNTABILITY - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party. A trusted system must be able to record the occurrences of security-relevant events in an audit log. The capability to select the audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis. Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations.

e. Requirement 5 - ASSURANCE - The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above. In order to assure that the four requirements of security policy, marking, identification, and accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions. These mechanisms are typically embedded in the operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such system mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency.

f. Requirement 6 - CONTINUOUS PROTECTION - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes. No computer system can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion. The continuous protection requirement has direct implications throughout the computer system's life cycle. These fundamental requirements form the basis for the individual evaluation criteria applicable for each evaluation division and class. The interested reader is referred to section 5 of the orange book, "Control Objectives for Trusted Computer Systems," for a more complete discussion and further amplification of these fundamental requirements as they apply to general-purpose information processing systems and to section 7 for amplification of the relationship between policy and these requirements.

804. STRUCTURE OF THE CRITERIA. The criteria are divided into four divisions: D, C, B, and A ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the most comprehensive security. Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information. Within divisions C and B, there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess. Assurance of correct and complete design and implementation for these systems is gained mostly through testing of the security-relevant portions of the system. The security-relevant portions of a system are referred to throughout this document as the Trusted Computing Base (TCB). Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. Increased assurance that the required features are operative, current, and tamper proof under all circumstances is gained through progressively more rigorous analysis during the design process.

a. Within each class, four major sets of criteria are addressed. The first three represent features necessary to satisfy the broad control objectives of security policy, accountability, and assurance that were discussed above. The fourth set, documentation, describes the type of written evidence in the form of user guides, manuals, and the test and design documentation required for each class.

b. The remainder of this chapter will delineate the requirements for FAA unclassified sensitive AIS such as payroll, CPMIS, UAS, and the ATC system. Details for the remaining division are contained in the orange book. The NSA/NCSC has determined that as a minimum a division C, class C2, is required for the above referenced AIS.

805. CLASS (C2): CONTROLLED ACCESS PROTECTION. Systems in this class enforce a more finely grained discretionary access control than Class (C1) systems, making users individually accountable for their actions through log-in procedures, auditing of security-relevant events, and resource isolation. The following are minimal requirements for systems assigned a Class (C2) rating:

a. Security Policy

(1) Discretionary Access Control. The TCB shall define and control access between named users and named objects (e.g., files and programs) in the AIS system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are prrtected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

(2) Object Reuse. All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

b. Accountability

(1) Identification and Authentication. The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Futhermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual AIS system user. The TCB shall also provide the capability of associating this identity with all audible actions taken by that individual.

(2) Audit. The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event,

the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events, the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The AIS system administrator or AISSO shall be able to selectively audit the actions of any one or more users based on individual identity.

c. Assurance.

(1) Operational Assurance

(a) System Architecture. The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the AIS system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

(b) System Integrity. Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the onsite hardware and firmware elements of the TCB.

(2) Life-Cycle Assurance. Security Testing. The security mechanisms of the AIS shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation or that would permit unauthorized access to the audit or authentication data. (See the Security Testing guidelines.)

d. Documentation.

(1) Security Features User's Guide. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) Trusted Facility Manual. A manual addressed to the AIS system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files, as well as the detailed audit record structure for each type of audit event, shall be given.

(3) Test Documentation. The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested and results of the security mechanisms' functional testing.

(4) Design Documentation. Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

e. Testing for Division C

(1) Personnel. Team members shall be able to follow test plans that are prepared by the system developer and suggest additions changes, etc to these plans, shall be familiar with the flaw hypothesis or equivalent security testing methodology, and shall have assembly level programming experience. Before testing begins, the team members shall have functional knowledge of, and shall have completed the system developer's internals course for, the system being evaluated.

(2) Testing. The team shall have "hands-on" involvement in an independent run of the tests used by the system developer. The team shall independently design and implement at least five system-specific tests in an attempt to circumvent the security mechanisms of the system. The elapsed time devoted to testing shall be at least 1 month and need not exceed 3 months. There shall be no fewer than 20 hands-on hours spent carrying out system developer-defined tests and test team-defined tests.

806. - 899. RESERVED.

CHAPTER 9. OFFICE AUTOMATION (OA) SYSTEMS

900. GENERAL. The use of personal computer systems (often called desk top or professional computers) within FAA has placed increasingly powerful information system technology in the hands of a growing number of users. While providing many benefits, the use of such small computer systems may introduce serious potential information security risks. Although considerable progress has been made in security management and technology for large-scale centralized data processing systems, relatively little attention has been given to the protection of small systems. As a result, significant exposures may exist which can threaten the confidentiality, integrity, or availability of information resources associated with such systems. To ensure effective protection of these valuable resources, managers, system designers, and users must be aware of the vulnerabilities which exist and control measures which should be applied.

901. SCOPE. This chapter is directed primarily to the use of microcomputers and word processors in FAA. Microcomputers and word processors will be classified as office automation (OA) systems. This includes desk-top, portable, and personal computers. When used wisely, these devices can significantly enhance the efficiency and effectiveness of FAA personnel and programs. When used in an unsecured fashion, however, sensitive information may be improperly handled. Each FAA employee who uses an OA system should be made aware of procedures and practices for its secure operation and maintain the security of the systems they are working with. The purpose of this chapter is to provide such guidance. Additional guidance can be obtained from the National Telecommunications and Information Systems Security (NTISS) Advisory Memorandum, titled, Office Automation Security Guideline, NTISSAM COMPUSEC/1-87 dated January 16, 1987.

902. RESPONSIBILITIES. There shall be one individual assigned responsibility for the security of each OA system. The individual will be the AIS Security Officer (AISSO). The individual should be one of the users of the system itself or may be a person who has responsibility for the security of all OA systems within a specified area. The AISSO has certain responsibilities which must be carried out in order to ensure that the OA security policy is enforced and appropriate security documentation is completed as required. These include:

a. Ensuring that all users of the system are aware of the security requirements and assuring that all procedures are being followed.

b. Ensuring that appropriate AIS security documentation is completed and forwarded to appropriate authorities (e.g., risk analysis, contingency planning, AIS security operating procedures, etc.)

c. Investigating all reported or suspected security violations and determining (to the best of his/her ability) what has happened.

d. Reporting violations to appropriate authorities (e.g., to management, AIS Security Coordinator.

e. Maintain an inventory of all assigned system hardware, firmware, and system and applications software.

In all cases, the level of security afforded an OA system shall be equivalent to the level of sensitivity of any information contained in or accessed by it. Classified information shall not be processed unless the procedures for classified processing contained herein are followed.

903. PROTECTING THE EQUIPMENT.

a. Protecting the OA system from theft and physical damage is not a fundamentally new problem; it has been necessary to protect office equipment for years. The only new factors are the relatively high unit value of OA systems and the need for somewhat greater concern for environmental controls. Otherwise, the physical protection needs of OA systems are the same as other valuable equipment in the workplace.

b. In general, OA systems should not be placed in areas which have no basic physical access controls (e.g., locks on the doors and people present during working hours). This is only prudent, since the value of a typical OA system may well be in excess of $2,000. Providing such simple and inexpensive controls will minimize not only the theft risk; it will also help reduce exposures to some of the more sophisticated technical problems.

c. OA systems which are located in unsecured areas must be equipped with a disabling device (such as a power-off lock) and a device to prevent physical removal and theft. Although this is not a requirement for OA systems located in secured areas, it is a recommended practice where money and resources are available. The cognizant security element can provide assistance in identifying and selecting appropriate physical security devices.

d. Where sensitive information is being processed, monitor screens, printers, and other devices that produce human-readable output shall not be viewable by casual observers or passers-by. OA systems shall not be left unattended while sensitive data is being processed unless the area is secured from unauthorized access.

904. ENVIRONMENTAL CONTROLS. OA systems are designed to operate in the "typical" office environment (i.e., without special air conditioning, electrical power quality control, or air contamination controls). In general, it can be argued that "if the people are comfortable, the OA system will be comfortable." Nevertheless, special attention should be given to minimizing the environmental hazards to which such equipment is exposed.

a. The introduction of an OA system does not represent any more of a significant fire hazard than does any other office equipment. It is unnecessary to install extensive fire and water protection systems similar to those required for major computer facilities as outlined in chapter 3. However, the value of the equipment, data, and other items in the area may be sufficient reason for reexamination of fire detection and suppression facilities. Smoking, eating, and drinking around the equipment should be restricted. In general good house keeping and file maintenance practices should be adhered to to preclude inadvertant loss of data.

b. If it is determined that fire extinguishing equipment is a cost-effective countermeasure, the guidelines in paragraph 363, shall be used.

905. REQUIREMENTS FOR CLASSIFIED PROCESSING. Facility or program managers who desire to use FAA stand alone OA systems to process classified information for either FAA or on behalf of another Federal agency shall request for system accreditation from the appropriate DAA. The request is to be submitted in the form of an accreditation document to the AISSC for review and recommendation. The accreditation documentation shall be prepared by the AISSO in accordance with Chapter 15 of this order. The request for accreditation shall identify each classified application processed. This document shall describe the AIS, the classification of data, the mode of operation, anticipated frequency of processing, and the applicable security measures implemented, in sufficient detail to permit a determination to be made as to their adequacy.

a. Classified data produced by an OA system must be stored on removable media and protected to the same degree as if it were produced manually. This means that it must be safeguarded, marked, controlled, transmitted, and destroyed with the same degree of security as if it were a manually processed document. Guidance on protecting classified information may be obtained from the cognizant security office, Order 1600.2B, National Security Information, and chapter 5.

b. OA systems which are used to process classified information shall not have communications capability (stand-alone only) and shall have documented system security procedures which:

(1) Include provisions for labeling AIS media with external classification markings and internal notations (sufficient to assure that any recipient of the media will know the specific classification level involved),

(2) Provide measures for an approved method of destruction for classified output and AIS media,

(3) Provide measures for controlling the distribution of the output and AIS media, and

(4) Provide measures preventing unauthorized access to the data.

906. PROTECTION OF STORAGE MEDIA. Where an OA system will be shared by different users who do not require access to all of the information contained in it and access cannot be controlled by passwords, removable storage media shall be used. Potential dangers and proper handling techniques for floppy disks shall be known to all users. Users shall ensure that the following techniques are implemented:

a. Always store in the protective jacket.

b. Protect from bending or similar damage.

c. Insert carefully into the drive mechanism.

d. Maintain an acceptable temperature range (50-125 degress fahrenheit).

e. Avoid direct contact with magnetic fields.

f. Do not write directly on diskette jacket or sleeve.

907. LABELING STORAGE MEDIA. Storage media must be labeled to reflect the sensitivity of the data contained. Any storage media which contains "For Official Use Only" information, proprietary information, or information covered under the provisions of the Privacy Act must be marked accordingly. Classified and other unclassified sensitive information shall not be stored on non-removable storage media. All storage media must be provided appropriate secure storage when not in use. In systems which have built-in, nonremovable storage media, the information shall be reviewed regularly (minimum of once a week) to verify that classified and other sensitive unclassified data is not resident. Special procedures should be developed to clear residual memory when the system is left unattended, being repaired, or is accessed by someone who does not require access to the information stored.

908. OPERATIONAL SECURITY. Certain commands which are common to OA systems can be misleading. Generally, commands to copy or delete files cannot be trusted. Often, when the command to copy a file from one diskette to another is given, other files or sensitive data are also copied. Generally, the delete, erase, or remove command simply removes the file name or address. The data itself may still be recovered. Users should be made aware of these vulnerabilities so that they operate the devices in a manner appropriate to the sensitivity of the data involved.

a. Systems which are connected to other devices may be illicitly accessed and files, applications, and software accessed or changed without it being apparent to the owner. OA systems should be turned off or disconnected when not in use.

b. There are a number of public domain programs and utilities available today. Discretion and testing shall be implemented prior to using such software. This type of software may contain programs or instructions specifically designed to capture or alter data (i.e., trap doors, time bombs, Trojan horse). If the tests prove the software to be reliable and useful, it may be used only if written approval is granted and signed by the division manager. This approval authority may not be delegated. If the division manager approves the use of the tested software, the name of the software must be identified and described in the accreditation document. A copy of the letter authorizing the use of that specific public domain software must accompany the request for accreditation to assure that the DAA is aware that potentially hazardous software is in use on the system.

c. FAA directives relative to the use of commercial software packages do not exist primarily because every software package contains a licensing agreement. These agreements are very explicit on what can and cannot be done with a particular package with regard to the number of copies allowed and how they can be used. These restrictions vary by vendor. The agreement places the user personally responsible for violations of software copyright or licensing agreements. The agreement represents a contractual agreement between the software user and provider. Anyone who purchases software has an opportunity to not use the software if the terms are not agreeable. Once the software package is opened, you have implied agreement with all of the terms contained therein. FAA will not defend anyone in violation of software licensing agreements.

d. All data, especially sensitive applications and files, should be backed up on a regular basis to ensure continuity of operation should the working media be damaged or destroyed. Backup data should be stored in a remote secure location to ensure its survival in case the working copy is destroyed.

909. PASSWORD PROTECTION. Where password capability is provided, passwords of six or more characters, preferably a mixture of numbers and letters, shall be used to make unauthorized access more difficult. The password selected shall not be identifiable to the individual (e.g., social security number, birth date, etc.) and shall not be written down. Since passwords may be overheard or otherwise discovered by unauthorized individuals, they should be changed at least annually, unless compromise is suspected or personnel change necessitate immediate change.

910. PROTECTION DURING REPAIR. All sensitive data and programs should be removed prior to the system being accessed for maintenance or repair. Service contracts should contain appropriate security-related provisions to ensure protection of sensitive information. In the event of a component failure; i.e., hard disk, the user must maintain the integrity of sensitive or classified data. In cases where a contractor must remove media to be repaired at a contractor site, the user must ensure that the maintenance contract reflects access to the highest level of data on the disk and the contractor can appropriately safeguard the data. If the data is recoverable, it must be returned to the user agency or the damaged disk must be destroyed by secure means to prevent loss or compromise.

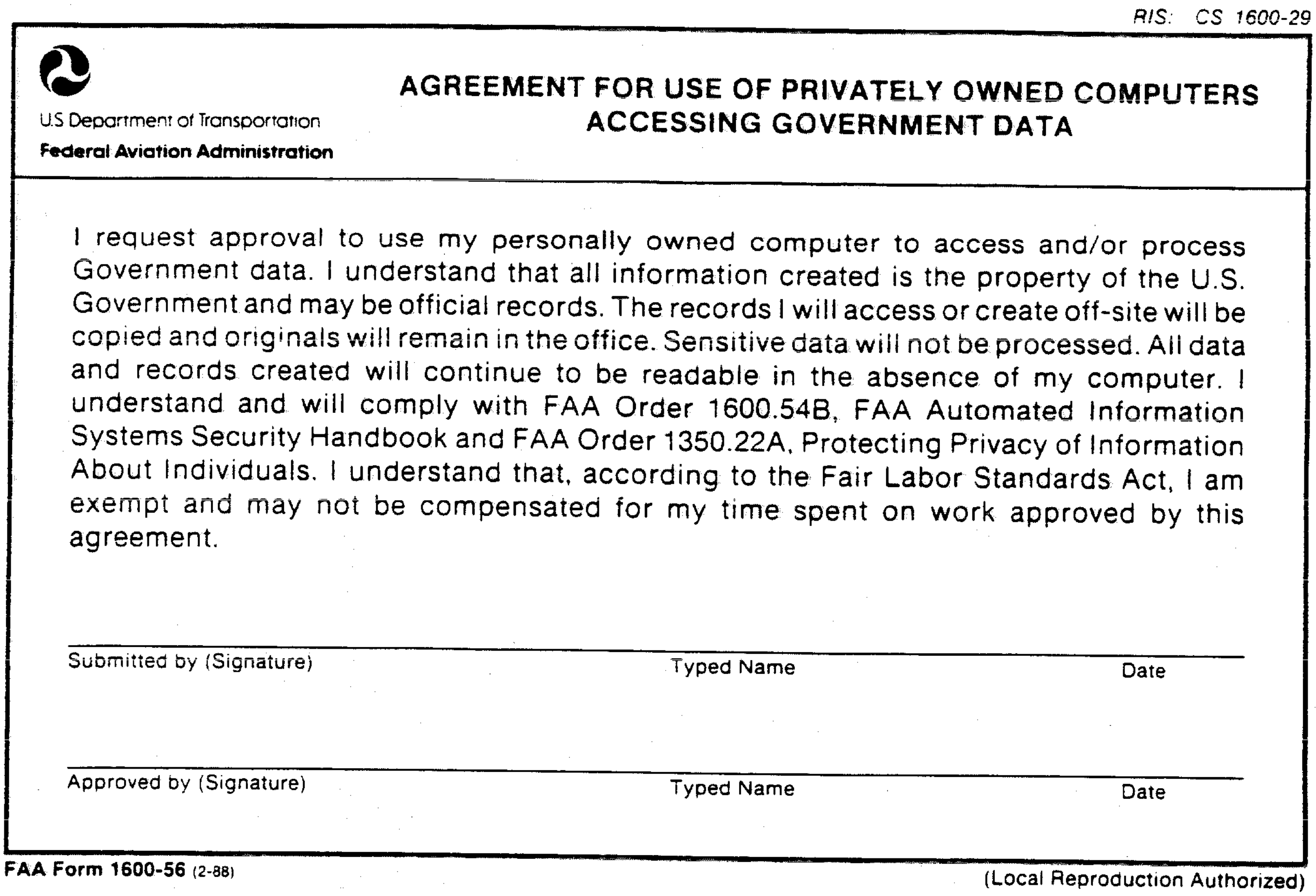
911. REQUIREMENTS FOR PRIVATELY OWNED OA SYSTEMS. Before an FAA employee uses a privately owned OA system on or off the work site to conduct Government business, permission must be granted by the AISSM. A copy of this permit shall be forwarded to the regional AIS Security Coordinator. Requests for permission should include justification, the period covered, and the applications which will be accessed. When permission is granted, a letter of agreement must be signed by the user and approving official. An agreement is shown in figure 9.1. Before an agreement is signed, the user must read and fully understand the policy outlined in figure 9.2. All data for Government jobs entered on OA systems, regardless of the ownership or location of the computers, are the property of the Government

and may be official records. This includes job-related work voluntarily done at home on privately owned computers. Such records are subject to Federal statutes and regulations, such as the Federal Records Act, Privacy Act, and the Freedom of Information Act. Government records created on privately owned computers must continue to be readable in the absence of that computer.

912. REQUIREMENTS FOR GOVERNMENT-OWNED OA SYSTEMS. Government-owned equipment, used on or off the work site, may only be used to conduct official business. Classified or sensitive data shall not be accessed or processed from off-site locations unless AIS security officials certify that the system and the data is adequately protected. Classified and sensitive data shall not be removed from the Government site. FAA activities shall establish or append property checkout procedures to ensure AIS equipment is properly controlled. A checkout procedure for diskettes and other media shall be established, and a backup copy of all records that are being removed shall be retained onsite.

913. - 999. RESERVED.

FIGURE 1. - LETTER OF AGREEMENT



RIS: CS 1600-29

U.S Department of Transportation
Federal Aviation Administration

AGREEMENT FOR USE OF PRIVATELY OWNED COMPUTERS ACCESSING GOVERNMENT DATA

I request approval to use my personally owned computer to access and/or process Government data. I understand that all information created is the property of the U.S. Government and may be official records. The records I will access or create off-site will be copied and originals will remain in the office. Sensitive data will not be processed. All data and records created will continue to be readable in the absence of my computer. I understand and will comply with FAA Order 1600.54B, FAA Automated Information Systems Security Handbook and FAA Order 1350.22A, Protecting Privacy of Information About Individuals. I understand that, according to the Fair Labor Standards Act, I am exempt and may not be compensated for my time spent on work approved by this agreement.

Submitted by (Signature) Typed Name Date

Approved by (Signature) Typed Name Date

FAA Form 1600-56 (2-88) (Local Reproduction Authorized)

Figure 9.2 - POLICY FOR FAA USE OF PRIVATELY OWNED COMPUTERS

FAA USE OF PRIVATELY OWNED COMPUTERS

It is the policy of FAA to permit employees to use privately owned microcomputers to work on Government business, subject to controls over records, property, and personnel.

Records created, stored, used, etc., on privately owned computers for official FAA business are the property of the Government and may be considered official records.

The FAA does not assume any responsibility for the safety, maintenance, security, or operation of the equipment, and the hardware, software, and data are subject to unannounced inspection.

Managers and supervisors will ensure that Government files and records created and used on privately owned computers for FAA activities will remain readable and accessible as needed by the Government. The user must understand and comply with the copyright laws as they pertain to software and computer operations.

Official FAA data and records shall be predicated upon the needs of the agency, not upon privately owned computers.

CHAPTER 10. CONTINGENCY PLANNING

1000. GENERAL. The preparation of a contingency plan is properly the responsibility of the AISSO. Both general and special purpose AIS's are critical to the accomplishment of FAA missions, the preparation of these plans enhance significantly the ability to minimize the impact of events having an adverse effect upon FAA AIS operations. Consequently, the creation of these plans becomes a key element in the FAA AIS Security Program. Contingency plans for all DPA's are required by OMB Circular Number A-130. NBS FIPS PUB #87 provides guidelines for contingency plan development. Within FAA, the development of these plans will require additional understanding of FAA facilities and their missions. Many DPA's within the FAA do not maintain an environment which will allow for normal contingency plan development as outlined in FIPS PUB #87. Appendix #4 is a sample outline of a contingency plan which may be adapted for a DPA which is involved with the control of aircraft traffic within the United States.

1001. SCOPE. The requirement for contingency plan development is applicable to all DPA's which house computer equipment used to support FAA operational or administrative missions for which unplanned disruption of service would have a critical impact on mission accomplishment. If unplanned disruption of services would not have a critical impact on mission accomplishment, the AISSM shall inform the regional AISSC, and no contingency plan is required.

1002. OBJECTIVE. The objective of the plan is to provide reasonable continuity of data processing support should events occur that prevent normal operations at the DPA. The plan must be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption or denial of service. A record and an assessment of the test shall be made with a statement of the corrective actions taken. The contingency plan shall provide a decision making process to be followed during or following the occurrence of unforeseen events impacting on normal AIS operations.

1003. CONDUCT DEVELOPMENT AND OF CONTINGENCY PLAN. Contingency plan development for FAA DPAs shall be accomplished by either the AISSO or the AISSM. Appendix 4 shall be used as a guideline and sample format. It is the responsibility of each AISSO to develop possible scenarios for each of the three subsections in the action plan. This part of the plan shall consist of the "what to" actions to be accomplished by the required personnel in the event of an emergency or disruption to service.

1004. DESIGNATION OF RESPONSIBILITY. The plan will designate responsibilities by position and not by employees. Individuals occupying or assuming a position shall sign and date a statement they have received orientation and/or reviewed the contingency plan annually.

1005.-1009. RESERVED.

CHAPTER 11. RISK ANALYSIS OF ALL DATA PROCESSING FACILITIES

1100. GENERAL. This chapter provides an overview of the risk analysis concepts as applied to data processing systems throughout the FAA. It additionally provides descriptive material regarding characteristics of the risk analysis methodology developed for FAA general purpose and special purpose computer systems. An outline of the management and administration of the FAA risk analysis program is also provided.

1101. RISK MANAGEMENT METHODOLOGY

a. An effective risk management program entails a four-phased evaluation effort such as the following:

(1) Risk assessment, as derived from an analysis of threats and vulnerabilities.

(2) Management decision.

(3) Control implementation.

(4) Effectiveness review.

b. Each of these phases should be applied to the areas of software, hardware, procedural, communications, emanations, personnel, and physical security. In addition, the relative risks within each area should be analyzed. Whenever possible, specialists should be used.

c. Since risk assessment involves expected loss based upon probabilities, the use of mathematical tools and statistical analysis would be a logical extension. Managers are cautioned, however, that attempts to develop absolute models, performance simulators, and/or descriptive algorithms have been only marginally successful. These techniques should be employed only when economically feasible and their value has been established.

1102. RISK ASSESSMENT ELEMENTS. The major components of a computer security risk assessment are:

a. RISK. A risk is derived from the analysis of a threat and a vulnerability. Formal risk assessment requires determination of relativity among risks and a perception of associated damage or loss. This relationship forms the basis for effective countermeasures. Risk assessment will be accomplished as part of the accreditation or reaccreditation of the DPA.

b. THREAT. A threat is considered to be any agent with a capability to reduce or neutralize the effectiveness of a system, thereby limiting or negating mission accomplishment. Threat identification is a difficult process which must consider both known and reliably postulated threats. Lack of evidence of threat agent activity can be expected since system penetration is difficult to detect by current audit procedures. Threats or threat agents include:

(1) Man-made or natural disaster, such as tornados, hurricanes, earthquakes, floods, lightning, windstorms, fire, rain, mud, ice, or snow.

(2) Deliberate or inadvertent error by authorized users such as programmers, operators, customers, librarians, management, and other personnel.

(3) "Hostile" agents, overt or covert, who could be unauthorized users of the system, part of the system, or an authorized user who attempts to misuse the system.

c. VULNERABILITY. System vulnerability is the total of susceptibilities to specific attack and the opportunity available to a hostile entity to mount that attack.

(1) General factors to be considered include-

(a) The geographical location.

(b) The operational and security modes.

(c) The sensitivity and amount of material being handled.

(d) Overall criticality of the mission or operation.

(2) The more complex the operation, the more susceptible the site. Local batch operations usually are less vulnerable than networked computers. The latter may be composed of large-scale, multiuser, online, shared operations which may be made more vulnerable depending upon the privileges extended to the users.

(3) Simple query privileges represent a lesser vulnerability potential than found in systems where the user has programming capability through use of a high-level query language or assembly or machine language. Vulnerabilities identified by inspection or notification and not corrected by the facility must be identified in all future risk assessments.

d. The determination of relative risk is a function of the management of the facility and the respective directorate or region. In many cases, the tolerable level of risk for a specific condition will be provided by FAA headquarters. Risk is most accurately adjudged when specific vulnerabilities are matched to known threats. This type of assessment usually produces more reliable information with which to qualitatively describe risk. In the absence of known threat, the vulnerability must still be evaluated for its potential effect since it may offer an opportunity for a hostile agent. The risk assessment process must assume that hostile agents are prepared to take advantage of significant system vulnerabilities.

1103. RISK ASSESSMENT FREQUENCY. Computer security risk assessments shall be accomplished under the following conditions, which are consistent with established OMB guidelines:

a. Prior to the approval of design specifications for new computer installations. This standard is for all computer facilities.

b. Whenever there is a significant change to the facility, hardware, system software, or application system. When a risk assessment is performed under conditions of significant change, only those threats, vulnerabilities, and risks relevant to the change need to be evaluated.

c. At least every 5 years.

1104. CONDUCT OF RISK ASSESSMENT. Risk assessments of FAA DPA's is the responsibility of the assigned AISSO or the AISSM of the DPI.

1105. TOOLS FOR RISK ASSESSMENTS.

There are two tools or methodologies for conducting risk assessments of FAA AIS. Both of these methodologies are user friendly and easy to accomplish. The AISSO assigned to a particular system is responsible for conducting the risk assessment, usually this person is most knowledgeable of the operation of the system, the associated security features and the environmental controls which are in place.

a. The Los Alamos Vulnerability Assessment (LAVA) is an automated tool to identify vulnerabilities of automated information facilities and to determine the level of risk. LAVA has been validated for FAA use from the National Computer Security Center (NCSC). LAVA is intended for the assessment of mainframe computer systems; however, it is run on a personal computer. Copies of the LAVA risk assessment methodology have been distributed to each FAA region/center security division. Further distribution will be made by the region/center AISSC as required.

b. Appendix 3, Short Form Risk Assessment, FAA Form 1600-57 (2-88), RIS: CS 1600-28, is a manual method for basic risk assessment. This risk assessment is suitable for AIS risk assessment for the personnel computer environment, office automation networks and other Office Automation (OA) systems as defined in paragraph 901. This is not considered an indepth methodology and should not be used as the sole element to determine the security posture of the AIS.

1106.-1119. RESERVED.

CHAPTER 12. CERTIFICATION OF SENSITIVE APPLICATIONS

1200. GENERAL. This chapter establishes the guidelines for certification of sensitive applications and designates the approval authority. NBS FIBS PUB 102, Guidelines for Computer Security Certification and Accreditation, provides further information on how to conduct the evaluations and certification.

1201. SCOPE OR CuNCEPTS. This chapter applies to all FAA sensitive applications. A risk analysis must be performed in order to certify a sensitive application system. If the sensitive application is a local (used by only one region/center), then its certification requires only the satisfactory risk analysis on that computer be accomplished. If the sensitive application is a national application (used by two or more regions or centers), then a risk analysis must be conducted for all DPA's involved before the certification can begin.

1202. OMB CIRCULAR NO. A-130 REQUIREMENTS. In accordance with OMB Circular No. A-130, all FAA sensitive applications will receive a security certification during their initial development. Operational sensitive applications will be recertified at least every 3 years. Operational sensitive applications that change significantly as defined in appendix 1 of this order will be recertified at the time of the change. Recertification process will follow the same guidelines of initial certification. Recertification must be performed parallel to operation.

1203. SECURITY CERTIFICATION RESPONSIBILITY AND AUTHORITY. Security certification is the approval and acceptance of responsibility of the security posture of an application system by the approving authority. Certification is based upon a security evaluation, risk analysis, and comparison of the level of established risk versus the cost of countermeasures. For national sensitive applications, the approval authority is the Director of Civil Aviation Security, ACS-1. For local sensitive applications, the approval authority is the regional/center AIS security manager. The certification is an acceptance of the risks outlined in the evaluation report. The certification approval authority may not be delegated.

1204. CERTIFICATION PROCESS. The factors to be considered for security certification must include all aspects of AIS security that are relevant to the application's environment, administrative, physical, technical areas, etc.

a. The certification evaluation must produce a certification evaluation report (figure 12-1) in order for the approval authority to make a certification decision.

b. The security evaluation will be assessed based on the criteria outlined at figure 12-2. This criteria is not all encompassing and is to be used only as a guide to things to be considered in making a certification decision.

c. A certification statement will be prepared once a decision has been made.

d. The certification statement (figure 12-3) will outline the factors that were considered during the evaluation. The certification statement, when signed, is an acceptance statement for the security posture of the sensitive application. This is accomplished after considering the risks involved and the countermeasures that are implemented.

1205. CERTIFICATION GUIDELINES. FIPS PUB 102 identifies the steps required to perform a computer security certification of an application. The major steps are organized as follows:

a. Planning. What preliminary steps are needed before primary evaluation activity can begin? How much evaluation depth is needed?

b. Information-Gathering Techniques. How is information gathered for evaluations?

c. Basic Evaluation. What is involved in performing a basic security evaluation for certification? What evaluation methods are applicable?

d. Detailed Evaluation. What is involved in a detailed evaluation? What methods are applicable to detailed evaluation? How can evaluation analysis be focused?

e. Evaluation Documentation. What does the security evaluation report contain?

f. Certification Decision. What issues are considered in making the certification decision? What does the certification statement contain?

g. Re-certification. When is recertification needed? What activities are involved? How are changes controlled?

Figure 12-4 is an outline for an Application Certification Plan.

1206.-1299. RESERVED.

FIGURE 12-1. Sample Outline for a Security Evaluation

1. Introduction and Summary

2. Background

3. Major Findings

   3.1 General Control Posture

   3.2 Vulnerabilities

4. Recommended Corrective Actions

5. Certification Process

Attachment A	Proposed Certification Statement
Attachment B (etc.)	Detailed Evaluation Report(s)

FIGURE 12-2. Criteria for Assessing Security Evaluation Reports

Resource Questions

1. What amount of resources (e.g., time, money) were expended in the evaluation?

2. Who performed the evaluation? What are their qualifications? Might there be any reasons to question their objectivity?

Process Questions

1. What technical review mechanisms were used?

2. Have the finding and recommendations been properly coordinated?

3. What major tools and techniques were used? What other experiences have there been with them? Have resources been effectively allocated to tools, analysis, and presentation of findings?

Content Questions

1. Based on the certifier's judgment, are the findings and recommendations reasonable?

2. What are other agencies doing in similar situations? Are Federal and agency requirements applicable to this application? Are there recent or proposed policy changes that are applicable? Do agency needs override user needs? What are the penalties for not complying with policies and requirements?

3. Did the evaluation focus on those things of primary importance? What assurances are there that major problem areas have not been overlooked? Are there safeguards not considered by the evaluation activity that might influence the findings? Are the recommendations prioritized? What was the basis for prioritization?

4. Many residual vulnerabilities will exist. Have they been identified?

5. Solitary quantitative final scores or ratings are unacceptable. Are recommendations and judgments supported? Is the quality of supporting data shown?

FIGURE 12-3. Illustrative Certification Statement

Subject: Certification of ______1______.
Reference computer security policies ______2______. This certification has been performed because ______3______.

I have carefully examined the evaluation findings and recommendations documented in the ______1______ security evaluation report, dated ____________. Based on my authority and judgment, I hereby certify (with the exceptions or clarification noted below) "That ______1______ meets the documented and approved security specifications, meets all applicable Federal policies, regulations, and standards, and that the results of (testing) demonstrate that the security provisions are adequate." 4

(exceptions or clarifications)

In addition, weighing the remaining residual risks against operational requirements, I have determined that (continued) operation of ______1______ (under the following restrictions) is in the agency's best interest:

(restrictions)

Accordingly, I hereby certify ______1______ to operate as described.

____
Signature and Date

1 Name of the application being certified.

2 OMB A-130, TMI and/or other applicable policies.

3 Reasons include the following: (1) initial development has been completed, (2) changes have been made, (3) requirements have changed, (4) a required threshold of time has been reached, (5) a major violation has occurred, and (6) audit or evaluation findings questions a previous certification.

4 Quotation from OMB A-130, TMI. The quotation marks are explanatory and are not included in the actual statement.

FIGURE 12-4 Sample Application Certification Plan Outline

1. Executive Summary

2. Introduction

    2.1 Background

    2.2 Scope

3. Responsibilities

    3.1 Evaluation Team

    3.2 Other Offices

4. Schedule

5. Support Required

    5.1 Administrative

    5.2 Technical

6. Evaluation Products

7. Tasks

Appendices

A. Certification

B. Tools to support technical evaluation (e.g. checklists)

CHAPTER 13. AIS SECURITY TRAINING AND AWARENESS

1300. GENERAL. AIS security training is a key element to the FAA AIS Security Program. Evaluating the risk within a DPA and implementing an effective AIS Security Program requires an increased consciousness of all FAA employees. An effective training and awareness program will provide both formal and informal instruction and, depending on the size and complexity of the DPA and the level of data being processed, will range from a security awareness program to a formalized AIS Security Training Program for all regional AISSC's and AISSO's.

1301. BACKGROUND. Automated Information Systems (AIS) are used throughout the FAA for many different purposes. These uses include the processing of information of a nonsensitive nature to the processing of extremely sensitive or classified information. The benefits and necessity of utilizing AIS are well recognized by FAA. Often overlooked or misunderstood are the risks that are inherent in the use of this beneficial equipment.

a. Data that is stored or manipulated electronically is more susceptible to loss than the traditional paper document. Loss may result from inadvertent user mistakes, exposure to magnetism, heat, water, exposure to sunlight and other agents that disrupt the magnetic storage integrity. Not only is electronic data more susceptible to loss, but the magnitude of the loss (amount of data) can be overwhelming and the speed at which the data is lost may be fractions of a second.

b. An additional risk inherent in the electronic storage or manipulation of data is the potential for unauthorized access or use of the data. Where the equipment is accessible via telecommunications, unauthorized use or access concerns must include the threat of unauthorized users gaining access.

1302. TRAINING RESPONSIBILITIES. Minimum training requirements have been established for the region/center AISSC. The manager, of the security element of the region and/or center is responsible for taking appropriate action to provide the AISSC with the training required. The AISSC is responsible for establishing a security awareness program. The program is to be implemented by the AISSM for each data processing installation (DPI).

1303. AISSC TRAINING REQUIREMENTS. The National AIS Security Program Manager (AISSPM) has established a formalized AIS security training curriculum. Each region and center AISSC will be required to attend the following courses:

a. Security in Automated Systems, ALMC-DX 87-06
U.S. Army Logistics Management Center
Fort Lee, Virginia 23801

b. Computer Security and Information Risk Management Course,
Department of Defense Computer Security Institute (DODCI)
Washington, DC 20374

1505. ACCREDITATION AUTHORITY.

a. Level I Data. The Administrator shall be the DAA for all AIS and networks processing Level I data. The regional administrators and center directors shall be the DAA for stand alone OA systems processing Level I data. The Director of Civil Aviation Security, ACS-1, shall be the DAA for stand alone OA systems processing Level I data at Washington headquarters.

b. Level II Data. The regional administrators and center directors shall be the DAA for all AIS, under their operational control, processing Level II data. The Director of Civil Aviation Security, ACS-1, shall be the DAA for AIS processing Level II data at Washington headquarters.

c. Level III Data. The AISSM shall be the DAA for all AIS processing Level III data at the DPI.

Figure 15-1 outlines the accreditation authority.

1506.-1599. RESERVED.

Figure 15-1. Accreditation Authority.

ACCREDITATION AUTHORITY
(DAA)

TYPE OF AIS

LEVEL	NATIONAL	REGIONAL	REGION/CENTER OA STAND ALONE	HQ OA STAND ALONE
I	AOA-1	AOA-1	REGIONAL ADMINISTRATOR/ CENTER DIRECTOR	ACS-1
II	ACS-1	REGIONAL ADMINISTRATOR/ CENTER DIRECTOR	REGIONAL ADMINISTRATOR/ CENTER DIRECTOR	ACS-1
III	N/A	N/A	AISSM	AISSM

APPENDIX 1. DEFINITION OF TERMS

The following definitions of terms are provided to assure their common understanding throughout FAA as they apply to the security of AIS and facilities.

Access. The ability and means to approach, to store or retrieve data, to communicate with or make use of any resources of an AIS system.

Access Category. One of the classes to which a user, a program, or a process in an AIS system may be assigned on the basis of the resources or groups of resources that each user, program, or process is authorized to use.

Access Control. The process of limiting access to the resources of an AIS system or communications network only to authorized users, programs, processes, or other AIS systems (in computer networks). Synonymous with controlled access, controlled accessibility. This is accomplished through the use of appropriate physical, procedural, and hardware/software controls.

Access Control Mechanism. Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an AIS system.

Access List. A catalogue of users, programs, or processes and the specifications of access categories to which each is assigned.

Access Period. A segment of time, generally expressed on a daily or weekly basis, during which access might prevail.

Access Type. The nature of an access right to a particular device, program, or file: for example, read, write, execute, append, modify, delete, create.

Accountability. The quality or state which enables violations or attempted violations of AIS system security to be traced to individuals who may then be held responsible.

Accreditation. The authorization and approval granted to an AIS system or network to process sensitive data in an operational environment, and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet prespecified technical requirements for achieving adequate data security.

Active Wiretapping. The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users.

Add-on Security. The retrofitting of protection mechanisms, implemented by hardware or software, after the AIS system has become operational.

Administrative Security. The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data. Synonymous with procedural security.

Automatic Data Processing. Data processing performed largely by automatic means; for example, by a system of electronic or electrical machines, including input, processing, and output operations.

AIS Activity. Any facility, installation, room, area, or building housing AIS equipment and where computer processing activities occur. Also see central computer complex.

AIS (Automated Information System). An assembly of computer equipment, facilities, personnel, software and procedures configured for the purpose of storing, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. For the purpose of this order, AIS systems are further categorized as:

a. General Purpose. This category includes all systems or processors used to support the management of FAA resources, perform administrative data processing function, or facilitate internal administrative communications.

b. Special Purpose. This category includes computer systems used in the actual or simulated control of air traffic, those used for the development of ATC software, and those which support ATC operations by performing communications processing and message switching functions.

AIS Security. The hardware/software functions, characteristics and features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; and the management constraints, physical structure, and devices; personnel and communications controls needed to provide an acceptable level of protection in a computer system.

AISSM - (Automated Information System Security Manager). This is the appointed individual responsible for Automated Information System Security for a DPI. The responsibilities are described in para 10j. of this order.

Analysis. See cost-risk analysis; cryptanalysis; risk analysis.

Approved Circuit. Synonym for protected wireline distribution system.

Audit.

a. To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

b. The independent review and examination of system activities and records as in paragraph 19a.

c. See external security audit; internal security audit; security audit.

Audit Trail. A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results

Authentication

a. The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

b. A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

Authenticator.

a. The means used to identify or verify the eligibility of a station, originator, or individual to access specific categories of information.

b. A symbol, a sequence of symbols, or a series of bits that are arranged in a predetermined manner and are usually inserted at a predetermined point within a message or transmission for the purpose of an authentication of the message or transmission.

Authorization. The granting to a user, a program, or a process the right of access.

Automated Security Monitoring. The use of automated procedures to ensure that the security controls implemented within an AIS system are not circumvented.

Backup Procedures. The provisions made for the recovery of data files and program libraries, and for the restart or replacement of AIS equipment after the occurrence of a system failure or of a disaster.

Between-the-lines Entry. Access, obtained through the use of active wire-tapping by an unauthorized user, to a momentarily inactive terminal of a legitimate user assigned to a communication channel.

Bounds Checking. Testing of computer program results for access to storage outside of its authorized limits. Synonymous with memory bounds checking.

Bounds Register. A hardware register which holds an address specifying a storage boundary.

Brevity Lists. A code system that is used to reduce the length of time required to transmit information by the use of a few characters to represent long, stereotyped sentences.

Browsing. Searching through storage to locate or acquire information, without necessarily knowing of the existence or the format of the information being sought.

Call Back. A procedure established for positively identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

Certification. The technical evaluation, made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system or network design and implementation meet a prespecified set of security requirements.

Central Computer Complex. The location in a single controlled room or area of one or more computers and their associated peripheral and storage units, central processing units and communications equipment and other related supporting resources essential to the operation of the system. Synonymous with central computer room, computer equipment room, or central computer facility.

Cipher System. A cryptographic system in which cryptography is applied to plain text elements of equal length.

Ciphertext. Unintelligible text or signals produced through the use of cipher systems.

Classified Information. Official information which requires protection against unauthorized disclosure in the interests of the national security of the United States, and which has been so designated in accordance with the provisions of E.O. 12356.

Closed Area. An area normally established to safeguard classified information and/or material

Code System.

a. Any system of communication in which groups of symbols are used to represent plain text elements of varying length.

b. In the broadest sense, a means of converting information into a form suitable for communications or encryption, for example, coded speech, Morse Code, tele-typewriter codes.

c. A cryptographic system in which crytographic equivalents (usually called code groups) typically consisting of letters, digits, or both in meaningless combinations are substituted for plain text elements which may be words, phrases, or sentences.

d. See also brevity lists.

Communications Security. The protection that ensures the authenticity of telecommunications, and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the interception of acquisition of telecommunications.

Compartmentalization.

a. The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs.

b. The breaking down of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

Compromise. An unauthorized disclosure or loss of sensitive information.

Compromising Emanations. Electromagnetic emanations that may convey data an that, if intercepted and analyzed, may compromise sensitive information being processed by any AIS system.

Computer. A mechanical or electronic apparatus which, by means of stored instructions and information, performs rapid, often highly complex, mathematical calculations or compiles, correlates, and selects data.

a. Computer Types. Computers can be digital, analog, or hybrid, which are defined as follows:

(1) Analog Computer. A computer using coded physical quantities, such as electrical resistance, voltage, etc., to solve problems, especially differential equations, an usually gives the solutions in the form of a graphic display, such as an oscilloscope pattern.

(2) Digital Computer. A computer using numbers, symbols, etc., consisting of coded digits to solve problems by means of arithmetic, especially in a binary system.

(3) Hybrid Computer. A computer using both analog and discrete representation of data. Also, it can be a digital and analog computer combined.

b. Computer Categories. As defined under "AIS System," for the purpose of this order, AIS systems were categorized as General and Special. However, a general or special computer could be a digital, analog, or hybrid computer. In addition, computer can be broken down into various categories. For the purpose of this order, the categories of general and special computers are defined as follows:

(1) Microcomputer. A category of stored program digital computers which are suitable for general purpose applications and are priced from under $1,000 up to $40,000. Additional characteristics include an individual power supply and enclosure, capability for attaching output peripherals such as a video screen and/or printer, as well as storage devices such as floppy diskettes, tape cassettes, or fixed disks. This category of computer is programmable in BASIC or equivalent level language.

(2) Minicomputer. The term "minicomputers" applies to the whole class of stored-program digital computers which are suitable for general purpose applications and are priced from $30,000 on up to about $80,000 in their minimum configurations. The typical minicomputer is a parallel, binary processor with a 16-bit word length (though 8-bit, 12-bit, 18-bit, 24-bit, and 32-bit word lengths are also fairly common). It uses integrated circuits and is housed in a compact cabinet suitable for either tabletop use or mounting in a standard 19-inch rack. It offers from 4,096 to 32,768 words of magnetic core or semi-conductor storage with a cycle time of 0.8 to 1.5 micro-seconds. Today's typical information minicomputer uses a one address instruction format and has two accumulators, a single index register, and a multilevel indirect addressing facility. Floating-point arithmetic requires the use of software sub-routines.

(3) Superminicomputer. A supermini, for the purposes of this order can generally be characterized as a computer that is distinguished by:

(a) A word length of more than 16 bits. A main storage capacity of one million bytes or more. An architecture that represents an extension of the architecture used in the vendor's smaller minicomputers. And a purchase price, for the basic CPU and minimum main storage, in the range of approximately $50,000 to $300,000.

(b) The great majority of the current superminis uses a 32-bit word length. A 32-bit word neatly holds four 8-bit bytes or two of the 16-bit words used in most of the smaller minicomputers. The 32-bit word length has been shown to yield an attractive balance between performance and cost in a broad range of applications. As a result, this word length has become so nearly universal among supermini designers that the terms "superminis" and "32-bit minicomputers" have become virtually synonymous.

(4) Memory Typewriter: Is a type of microcomputer that permanently or temporarily stores data on a tape or disk.

(5) Large Mainframe Computer.

(a) MainFrame. The mainframe of a computer system is the cabinet that houses the central processor unit (CPU) and main memory. It is, therefore, separate from the peripheral devices (card readers, printers, tape drives, etc.) and device controllers. Typically, it is the largest component in size and cost, but modern electronics have allowed great reductions in both in recent years. The term "mainframe" comes from the use of "frame" as a device to hold electronics (rack is also frequently used); and the frame holding the electronics that do the computing might reasonably be the mainframe. In modern systems with very large main memory, some memory modules are housed in cabinets separate from the mainframe. Frequently, they are attached and thus become part of the mainframe cabinet. Multiprocessor systems with more than one CPU are referred to as two or three mainframe systems, in which case the mainframe refers only to the CPU and not to the main memory.

(b) Central Processing Unit (CPU). The name "Central Processor" or central processing unit (CPU), is used to describe elements that carry out a variety of essential data manipulations and controlling tasks at the heart of the computer. Probably the most obvious element is the one required to carry out arithmetic and other operations on data, which is usually called the "arithmetic unit." The other obvious element is the control unit, required to supervise the functioning of the machine as a whole, calling into operation the various units as required by the program. It receives the program instruction one by one in sequence, interprets them, and sends appropriate control signals to the various units.

(c) Main Memory. Different levels of storage (or memory) are usually employed in a computer system. Two important characteristics of main memory are: (1) The main memory is a read/write memory (RW or R/W) permitting data to be stored or retrieved at comparable intervals. (2) The main memory is a random access memory (RAM); i.e., the time to access each stored word is constant, independent of the sequence in which words were stored. This should be contrasted with serial memories such as disks, drums, tapes, and shift registers in which data is available only in the same sequence as originally stored.

(5) Plug-Compatible Mainframe. The plug-compatible mainframe (PCM) industry was launched several years ago with the installation of the first Amdahl 470V/6 system. The acknowledgement that the IBM system/360 and System/370 instruction set has become a de facto standard for the industry, and that requires extensive reprogramming. The primary thrust of the PCM manufacturers has been to provide cost-effective alternatives to the IBM system 370, 303X Series, 3081, and 4300 series computers. Plug-compatible mainframes are typically defined as computer mainframes that can directly execute all application programs and systems software written for the IBM system 370, 303X Series, 308X Series, and/or 4300 Series computers and can utilize the peripheral equipment available for these computers.

Concealment system. A method of achieving confidentiality in which the existence of sensitive information is hidden by embedding it in irrelevant data.

Confidentiality. A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provide for such data about individuals as well as organizations.

Controlled security mode. The mode of operation that is a type of multilevel security mode in which a more limited amount of trust is placed in the hardware/software base of the system, with resultant restrictions on the classification levels and clearance levels that may be supported.

Control Zone. The space expressed in feet of radius, that surrounds equipment that is used to process sensitive information and this is under sufficient physical and technical control to preclude an unauthorized entry or compromise. Synonymous with security perimeter.

Controlled Access. Synonym for access control

Controlled Accessibility. Synonym for access control.

Controlled Sharing. The condition which exists when access control is applied to all users and components of a resource-sharing AIS system.

Controllable isolation. Controlled sharing in which the scope or domain of authorization can be reduced to an arbitrarily small set or sphere of activity.

Cost-risk Analysis. The analysis of the costs of potential risk of loss of compromise of data in an ADP system without data protection versus the cost of providing data protection.

Cross-Talk. An unwanted transfer of energy from one communications channel to another channel.

Cryptanalysis. The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption algorithm.

Cryptographic System. The documents, devices, equipment, and associated techniques that are used as a unit to provide a single means of encryption (enciphering or encoding).

Cryptography. The art or science which treats of the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

Cryptology. The field that encompasses both cryptography and cryptanalysis.

Crypto-operation. A deliberate or accidental process or act that results in a change in the integrity of the original data.

Data-dependent Protection. Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file which includes the data elements.

Data Integrity. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Data Processing Installation (DPI). This is one or more DPA (computers) located in:

a. An office (for example, the Office of Management Systems in Washington)

b. A division (for example, the Personnel Division in a region or center.

c. A facility (for example an automated FSS or ARTCC)

Data Processing Activity (DPA). This is a single computer which may be composed of multipieces of equipment, e.g., printer, disk drive, tape drive, CPU, control unit, etc. or it could be a stand alone microcomputer with no printer such as a portable Grid computer.

An example of a DPI, such as an ARTCC could have the following defined as DPA's within the DPI:

IBM 9020, IBM 3083, TANDEM, COMPUSTAR, APOLO, Lee Data

Data Security. The protection of data from accidental or malicious modification, destruction, or disclosure.

Data protection engineering. The methodology and tools used for designing and implementing data protection mechanisms.

Decipher. To convert, by use of the appropriate key, enciphered text into its equivalent plain text.

Decrypt. To convert, as in converting from encrypted text to plain text.

Degauss.

a. To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media, usually tapes. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media.

b. Loosely, to erase.

Eavesdropping. The unauthorized interception of information-bearing emanations through the use of methods other than wiretaping.

Electromagnetic Emanations. Signals transmitted as radiation through the air and through conductors.

Emanation Security. The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations.

Emanations. See compromising emanations; electromagnetic emanations.

Encipher. To convert plain text into unintelligible form by means of a cipher system.

Encode. To convert plain text into unintelligible form by means of a code system.

Encrypt. To convert plain text into unintelligible form by means of a cryptographic system.

Encryption. See end-to-end encryption; link encryption.

Encryption Algorithm. A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations through the use of variable elements controlled by the application of a key to the normal representation of the information. Synonymous with privacy transformation.

End-to-end Encryption.

a. Encryption of information at the origin within a communications network and postponing decryption to the final destination point.

b. See also link encryption.

Entrapment. The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit.

Entry. See between-the-lines entry; piggy back entry.

Executive State. One of two generally possible states in which an AIS system may operate, and in which only certain privileged instructions may be executed; such privileged instruction may not be executed when the system is operating in the user state. Synonymous with supervisor state.

External Security Audit. A security audit conducted by an organization independent of the one being audited.

Failure Access. An unauthorized and usually inadvertent access to data resulting from a hardware or software failure in the AIS system.

Failure Control. The methodology used to detect and provide fail-safe or fail-soft recovery from hardware and software failures in an AIS system.

Fail Safe. The automatic termination and protection of programs or other processing operations when a hardware or software failure is detected in an AIS system.

Fail Soft. The selective termination of affected nonessential processing when a hardware or software failure is detected in an AIS system.

Fault. Synonym for loophole

Fetch Protection. A system-provided restriction to prevent a program from accessing data in another user's segment of storage.

File protection. The aggregate of all processes and procedures established in an AIS and designed to inhibit unauthorized access, contamination, or elimination of a file.

Flaw,

a. Synonym for loophole.

b. See pseudo-flaw

Formulary. A technique for permitting the decision to grant or deny access to be determined dynamically at access time, rather than at the time of creation of the access list.

"For Official Use Only" (FOUO) Information. That nonclassified official information of a sensitive, proprietary, or personally private nature which must be protected against unauthorized public release, in accordance with the provisions of Order 1600.15D. See also sensitive information.

Handshaking Procedures. A dialogue between a user and a computer, a computer and another computer, a program an another program for the purpose of identifying a user and authenticating his identity, through a sequence of questions and answers based on information either previously stored in the computer or supplied to the computer by the initiator of dialogue. Synonymous with password dialogue.

Hardware Security. Computer equipment features or devices used in an AIS system to preclude unauthorized access to data or system resources.

Identification. The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to an AIS system.

Impersonation. An attempt to gain access to a system by posing as an authorized user. Synonymous with masquerading, mimicking.

Incomplete Parameter Checking. A system fault which exists when all parameters have not been fully checked for correctness and consistency by the operating system, thus making the system vulnerable to penetration.

Integrity. See data integrity; system integrity.

Interactive Computing. Use of a computer such that the user is in control and may enter data or make other demands on the system which responds by the immediate processing of user request and returning appropriate replies to these requests.

Interdiction. The act of impeding or denying the use of system resources to a user.

Internal Security Audit. A security audit conducted by personnel responsible to the management of the organization being audited.

Isolation. The containment of users and resources in an AIS system in such a way that users and processes are separate from one another as well as from the protection control of the operating system.

Key. In cryptography, a sequence of symbols that controls the operations of encryption and decryption.

Key Generation. The origination of a key or of a set of distinct keys

Keyword. Synonym for password.

Linkage. The purposeful combination of data or information from one information system with that from another system in the hope of deriving additional information; in particular, the combination of computer files from two or more sources.

Link Encryption.

a. The application of online crypto-operations to a link of communications system so that all information passing over the link is encrypted in its entirety.

b. End-to-end encryption within each link in a communications network

Lock-and-key Protection System. A protection system that involves matching a key or password with a specified access requirement.

Logical Completeness Measure. A means for assessing the effectiveness and degree to which a set of security and access control mechanisms meets the requirements of a set of security specifications.

Loophole. An error of omission or oversight in software or hardware which permits circumventing the access control process. Synonymous with fault, flaw.

Masquerading. Synonym for impersonation.

Memory Bounds. The limits in the range of storage addresses for a protected region in memory.

Memory Bounds Checking. Synonym for bounds checking.

Mimicking. Synonym for impersonation.

Monitoring. See automated security monitoring; threat monitoring.

Multiple Access Right Terminal. A terminal that may be used by more than one class of users; for example, users with different access right to data.

Mutually Suspicious. Pertaining to the state that exists between interactive processes (subsystems or programs) each of which contains sensitive data and is assumed to be designed so as to extract data from the other and to protect its own data.

Nak Attack. A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and, thus, leaves the system in an unprotected state during such interrupts.

Offline Crypto-operations. Encryption or decryption performed as a self-contained operation distinct from the transmission of the encrypted text, as by hand or by machines not electrically connected to a signal line.

Online Crypto-operation. The use of crypto-equipment that is directly connected to a signal line, making single continuous processes of encryption and transmission or reception and decryption.

Operating System (O/S). An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other system-related function.

Operational Data Security. The protection of data from either accidental, unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

Overwriting. The obliteration of recorded data by recording different data on the same surface.

Passive Wiretapping. The monitoring and/or recording of data while the data are being transmitted over a communications link.

Password. A protected word or string of characters that identifies or authenticates a user, a specific resource, or an access type. Synonymous with keyword.

Password Dialogue. Synonym for handshaking procedure.

Penetration. A successful unauthorized access to an AIS.

Penetration Profile. A delineation of the activities is required to effect a penetration.

Penetration Signature.

a. The description of a situation or set of conditions in which a penetration could occur.

b. The description of usual or unusual system events which in conjunction can indicate the occurrence of a penetration in progress.

Penetration Testing. The use of special programmer/analyst teams to attempt to penetrate a system for the purpose of identifying any security weaknesses.

Personnel Security. The procedures established to ensure that all personnel who have access to any sensitive information have the required authorities as well as the appropriate clearances.

Physical Security.

a. The use of locks, guards, badges, and similar administrative measures to control access to the computer and related equipment.

b. The measures required for the protection of the structures housing the computer, related equipment, and their contents from damage by accident, fire, and environmental hazards.

Piggy Back Entry. Unauthorized access that is gained to an AIS system via another user's legitimate connection.

Plain Text. Intelligible text or signals that have meaning and that can be read or acted upon without the application of any decryption.

Principle of Least Privilege. The granting of the minimum access authorization for the performance of required tasks.

Print Suppress. To eliminate the printing of characters in order to preserve their secrecy; for example, the characters of a password as it is keyed by a user at an input terminal.

Privacy. The concept embodying the desire by an individual to determine for himself when, how, and to what extend information about him can be obtained or communicated to others. Privacy also includes the right of individuals to know that recorded information is accurate, pertinent, complete, up-to-date, and reasonably secure form unauthorized access--either accidental or intentional.

Privacy Protection. The establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of data records and to protect both security and confidentiality against any anticipated threats for hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

Privacy Transformation. Synonym for encryption algorithm.

Privileged Instructions.

a. A set of instruction generally executable only when the AIS is operating in the executive state; for example, the handling of interrupts.

b. Special computer instructions designed to control the protection features of an AIS system; for example, the storage protection features.

Procedural Security. Synonym for administrative security.

Procedures. See backup procedures; handshaking procedures; recovery procedures; system integrity procedures.

Protected Wireline Distribution System. A telecommunications system which has been approved by a legally designated authority and two which electromagnetic and physical safeguards have been applied to permit safe electrical transmission of unencrypted sensitive information. Synonymous with approved circuit.

Protection. See data-dependent protection; fetch protection; file protection; lock-and-key protection system; privacy protection.

Protection Ring. One of a hierarchy of privileged modes of an AIS that gives certain access right to the users, programs and processes authorized to operate in a given mode.

Pseudo-flaw. An apparent loophole deliberately implanted in an operating system program as a trap for intruders.

Purging.

a. The orderly review of storage and removal of inactive or obsolete data files.

b. The removal of obsolete data by erasure, by overwriting of storage, or by resetting registers.

Real-time Reaction. A response to a penetration attempt which is detected and diagnosed in time to prevent the actual penetration.

Recovery Procedures. The actions necessary to restore a system's computational capability and data files after a system failure or penetration.

Remanence. The residual magnetism that remain on magnetic storage media after degaussing.

Remote Terminal Room. An enclosed area or room which houses one or more remote terminals or remote job entry devices. Synonymous with terminal cluster room.

Residue. Data left in storage after processing operations, and before degaussing or rewriting has taken place.

Resource. In an AIS, any function, device, or data collection that may be allocated to users or programs.

Resource Sharing. In an AIS, the concurrent use of a resource by more than one user, job, or program

Restricted Area. A room, area, or facility having critical activities, equipment, or information to which unrestricted access cannot be allowed for reasons of safety, operational necessity, or the need to protect the data processed or stored within the area.

Risk. The probability or likelihood of a given loss or damage to a particular system, facility, or major application.

Risk Analysis. The process of evaluating identified threats to determine their impact upon the AIS, facility, operation and upon supported organizations or other users. The objective of a risk analysis is to assess the severity of risk and weigh the expected losses that they may be ranked according to degree of acceptability or unacceptability. There are three types of risk analysis that may be conducted simultaneously or independently.

a. Comprehensive. A risk analysis that includes both facility and system/application reviews.

b. Facility. This type of risk analysis is oriented towards the threats against the DPA.

c. System/Application. This category of risk analysis is directed at the threats against sensitive and/or critical files and/or applications.

Risk Management. An element of management science concerned with identifying, measuring, and minimizing the effects of untoward events. The objective of the risk management process is to enable AIS operations to be conducted within an environment of acceptable risk to losses through destruction, delay, disclosure, and modification. When applied to the security of computer operations, risk management encompasses:

a. Risk analysis;

b. Management Decision;

c. Control Implementation; and

d. Effectiveness Review.

Sanitizing. The degaussing or overwriting of sensitive information in magnetic or other storage media. Synonymous with scrubbing.

Scavenging. Searching through residue for the purpose of unauthorized data acquisition.

Scrubbing. Synonym for sanitizing.

Secure Configuration Management. The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that such changes will not lead to a decreased data security.

Secure Operating System. An operating system that effectively controls hardware and software function in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system.

Security. See add-on security; administrative security; communications security; data security; emanation security; personnel security; physical security; procedural security; teleprocessing security; traffic flow security.

Security Audit. An examination of data security procedures and measures for the purpose of evaluating their adequacy and compliance with established policy.

Security Filter. A set of software routines and techniques employed in AIS to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons.

Security Incidents. Any incident involving the penetration, user subversion, compromise of classified or sensitive information, unauthorized use access or storage of information which is a violation of the requirements, procedures or directives of Government agencies (e.g. fraudulent use of systems or information, inadvertent disclosure, unauthorized access to a Central Computer Room or computer system from a remote terminal).

System Inventory Directory. A listing of all systems used at a facility or DPI to include software systems and hardware of systems.

Sensitive Data. Data that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

Sensitive Information System. A system that processes sensitve data.

Significant Change. To determine the need for conducting or revising a risk analysis, this term is defined as follows:

a. Significant Physical Facility Change. If any of the following conditions are met, the change is significant:

(1) Introducing new construction, remodeling, or new activities in building areas contiguous to rooms containing AIS hardware or supporting functions that potentially increases the hazards of accidents or natural disasters.

EXAMPLES: Constructing a cafeteria one floor below a computer room in a flood plain, removing a nearby levee; storing flammable materials near a data communications room.

(2) Making any modification to the physical operating environment of an AIS that removes or relaxes existing physical security controls.

EXAMPLES: Shutting off the water main to sprinkler system; putting in a new door to the computer room without controlling access.

b. Significant Hardware Change. If any of the following conditions are met, the change is significant:

(1) Adding or replacing any AIS hardware or other supporting equipment that increases the AIS tangible assets of the facility by more than $500,000 in a single fiscal year.

EXAMPLES: Purchasing and installing a new $550,000 mainframe; adding disk storage units of $400,000 and a telecommunications facility of $120,000 in a single fiscal year.

(2) A condition that causes an item of AIS hardware or other supporting equipment necessary for the continued operation of the facility to be irreplaceable if destroyed. Also, the condition is met if replacement is likely to take longer than current contingency planning can tolerate.

EXAMPLES: Requiring replacement of a critical computer component that is no longer supplied or produced by the vendor; absence of sufficient spare components or parts to replace a unique item.

(3) Any hardware modification, replacement, or addition that relaxes or removes controls over existing system access, over operational or administrative procedures, or over input/output media.

EXAMPLES: Replacing a Central Processing Unit (CPU) with one of another vendor that has fewer security features; replacing direct access disk storage by another mass storage device that changes the access rules and procedures by computer room personnel.

c. Significant System Software Change. If any of the following conditions are met, the change is significant:

(1) Adding, modifying, or replacing any system software, utility, data base management system, or other similar program or module not part of routine system maintenance or scheduled vendor relapses that involves over $50,000 or 1 person-year of effort in a single fiscal year.

EXAMPLES: Rewriting a module of the operating system that consumes 13 person months of effort in a single fiscal year.

(2) Adding, modifying, or replacing any system software, utility data base management system, or other similar program or module that relaxes or removes identification,authentication, system access, procedural, or other data security controls.

EXAMPLES: Removing system access passwords; replacing a data base management system having file access codes with one that does not.

(3) Adding, modifying, or replacing any system software, utility, data base management system, or other similar program or module that increases the system capabilities of users, programmers, or other individuals previously not possessing those capabilities on the AIS system to access, modify, or delete.

EXAMPLES: Adding system dialup telecommunications for remote batch processing; replacing batch programming with an interactive coding/debugging facility.

d. Significant Application Change. If any of the following conditions are met, the change is significant:

(1) Adding, modifying, or replacing any application system software or related program that consumes more that 1 person-year of effort or costs more than $50,000 in a single fiscal year, other than routine or scheduled maintenance.

(2) Adding, modifying, or replacing any application system software or related program that relaxes or removes identification, authentication, system access, procedural, or other application system controls.

(3) Increasing the volume of input, output, or distribution by 30 percent or more, or increasing the dollar value of the assets controlled in the application by $100 million within a single fiscal year.

EXAMPLES: Adding a new subsystem to an inventory control application, under contract for $60,000; removing audit trails from payroll transaction; consolidating a new group of FAA employees into a payroll system, with the new group adding $1,200,000 to the annual gross payroll.

Software Security. Those computer programs and routines which protect data or information processed by an AIS system and its resources.

Spoofing. The deliberate inducement of a user or a resource to take an incorrect action.

Standalone Office Automation System. An OAS having no telecommunications or connectivity to another AIS.

Storage. Component or device in which data can be stored and retrieved by a computer.

Supervisor State. Synonym for executive state.

System. See cipher system; code system; concealment system; cryptographic system; lock-and-key protection system; protected wireline distribution system; secure operating system.

System Integrity. The state that exists when there is complete assurance that under all conditions an AIS is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanism, and data integrity.

System Integrity Procedures. Procedures established for assuring that the hardware, software, and data in an AIS maintain their state of original integrity and are not tampered with by program changes.

Technological Attack. An attack which can be penetrated by circumventing or nullifying hardware and software access control mechanisms, other than by subverting system personnel or other users.

Telecommunications. Any transmission, emission, or reception of signs, signals, writing, images, sounds, or other information by wire, radio, visual, or any electromagnetic systems.

Teleprocessing. Pertaining to an information transmission system that combines telecommunications, AIS, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole.

Teleprocessing Security. The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system.

Terminal Area. An area that may consist of one or more terminals connected to a computer either by the use of a modern or hard wire. If microcomputers are used for terminals then when the microcomputer is used as a stand alone device it is considered a Data processing activity.

Terminal Identification. The means used to establish the unique identification of a terminal by an AIS system.

Threat. The source of an adverse event that can cause a loss. Threats are categorized into (a) natural hazards, (b) accidents, and (c) intentional acts.

Threat Monitoring. The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events which may constitute violations or precipitate incidents involving data privacy matters.

Time-dependent Password. A password which is valid only at a certain time of the day or during a specified interval of time.

Traffic Flow Security. The protection that results from those features in some crypto-equipment that conceal the presence of valid messages on a communications circuit, usually by causing the circuit to appear busy at all times, or by encrypting the source and destination addresses of valid messages.

Trap Door. A breach created intentionally in an AIS for the purpose of collecting, altering, or destroying data.

Trojan Horse. A computer program that is apparently or actually useful that contains a trap door.

User. Any authorized person, office, or facility that may directly enter into or receive from a computer system data.

Validation. The performance of tests and evaluations in order to determine compliance with security specifications and requirements.

Vulnerability. Any weakness or flaw existing in the protective mechanism provided for an AIS, DPA, or operation.

Wiretapping. See active wiretapping, passive wiretapping.

Work Factor. An estimate of the effort or time that can be expected to be expended to overcome a protective measure by a would-be penetrator with specified expertise and resources.

APPENDIX 2. RELATED DIRECTIVES AND STANDARDS

The following Federal standards and FAA/DOT orders also are relevant to the subject of ADP security.

1. Federal Regulations and Guidelines.

a. OMB Circular No. A-130, "Management of Federal Information Resources". December 12, 1985.

b. OMB Circular No A-123, "Internal Control Systems". March 9, 1982

c. NBS FIPS PUB 31, Guidelines for Automated Data Processing Physical Security and Risk Management. June, 1974

d. NBS FIPS PUB 38, Guidelines for Documentation of Computer Programs and Automated Data Systems. February 15, 1976

e. NBS FIPS PUB 39, Glossary for Computer Systems Security. February 15, 1976

f. NBS FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974. May 30, 1975

g. NBS FIPS PUB 46, Data Encryption Standard. January 15, 1977

h. NBS FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification. April 1, 1977

i. NBS FIPS PUB 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase. August 1, 1979

j. NBS FIPS PUB 65, Guidelines for Automated Data Processing Risk Analysis. August 1, 1979

k. NBS FIPS PUB 73, Guidelines for Security of Computer Applications. June 30, 1980

l. NBS FIPS PUB 76, Guidelines for Planning and Using a Data Directory System. August 20, 1980

m. NBS FIPS PUB 77, Guidelines for Planning and Management of Database Applications. September 1, 1980

n. NBS FIPS PUB 83, Guidelines on User Authentication Techniques for Computer Network Access Control. September 29, 1980

p. NBS FIPS PUB 87, Guidelines for ADP Contingency Planning. March 27, 1981

q. NBS FIPS PUB 88, Guidelines on Integrity Assurance and Control in Database Administration. August 14, 1981

r. RP-1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations. August 1978

s. 29 CFR 1910, OSHA Standards for General Industry. April 1, 1981

t. 34 CFR 281, ADP Management Information System (ADP/MIS). May 1, 1976

u. 34 CFR 282, Management, Acquisition and Utilization of Automatic Data Processing (ADP). June 1, 1976

v. Federal Property Management Regulation 101-36.7, Environmental and Physical Security. June, 1981

w. Federal Property Management Regulation 101-36.12, Care and Handling of Magnetic Computer Tape. June, 1978

2. FAA Orders.

a. Order 1000.32, Internal Control Systems, September 20, 1982

b. Order 1350.22A, Protecting Privacy of Information about Individuals, January 7, 1982

c. Order 1370.32B, Use of Computer Time Sharing Services, May 8, 1979

d. Order 1370.43, Computer Time-Sharing Users Guide for FAA Personnel, November 29, 1972

e. Order 1370.48, Automated Data Systems and Automatic Data Processing, March 11, 1976

f. Order 1370.52B Information Resources Management Policy and Procedures, August 27, 1984

g. Order 1370.53, Uniform Documentation Standards for the Development, Maintenance, Operation of Automated Data Systems, April 28, 1977

h. Order 1600.1C, Personnel Security Program, May 1, 1973

i. Order 1600.2B, National Security Information, February 5, 1980

j. Order 1600.6B, Protection of Agency Property, August 25, 1978

k. Oruer 1600.8B, Communications Security, November 1, 1975

l. Order 1600.15D, Control and Protection of "For Official use Only" Information, September 6, 1972

m. Order 1600.39A, Removal of Equipment from DOT Buildings, November 14, 1974

n. Order 1600.40, Security for Electrically Transmitted Messages, September 1, 1972

o. Order 1600.46, Physical Security Review of New Facilities, Office Space or Operating Areas, July 14, 1975

p. Order 1600.49B, Security Classification of Joint-Use Radar Information, May, 1988

q. Order 3900.19A, Occupational Safety and Health, July 20, 1982

r. Order 6930.1A, Fire Prevention and Maintenance of Fire Protection Equipment, Reprinted November 13, 1978 (includes changes 1 thru 2)

3. DOT Orders.

a. Order DOT 1370.48, Automatic Data Processing Management Policy, January 17, 1975

b. Oruer DOT 1640.7, Department of Transportation Automatic Data Processing Security Policy, July 9, 1976

c. Order DOT 1640.8, Department of Transportation Automatic Data Processing Security, November 12, 1976

4. Miscellaneous.

a. NBS Technical Note (TN) 735, The Effects of Magnetic Fields on Magnetic Storage Media Used in Computers, July 1972

b. NBS TN 730, Controlled Accessibility Bibliography, June 1973

c. NBS TN 809, Government Look at Privacy of Security in Computer Systems, February 1974

d. NBS TN 827, Controlled Accessibility Workshop Report, May 1974

e. NBS Special Publications (SP) 404, Approaches to Privacy and Security in Computer Systems, September 1974

f. NBS SP 500-9, The Use of passwords for Controlled Access to Computer Resources, May, 1977

g. NBS SP 500-19, Audit and Evaluation of Computer Security, October, 1977

h. NBS SP 500-27, Computer Security and the Data Encryption Standard, February, 1978

i. NBS SP 500-54, A Key Notarization System for Computer Networks, October, 1979

j. NBS SP 500-57, Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, April, 1980

k. NFPA Standard No. 10, Standard for the Installation of Portable Fire Extinguishers.

l. NFPA Standard No. 12, Carbon Dioxide Extinguishing Systems.

m. NFPA Standard No. 12A, Halogenated Extinguishing Agent Systems-Halon 1301.

n. NFPA Standard No. 13, Installation of Sprinkler Systems.

o. NFPA Standard No. 70, National Electrical Code.

p. NFPA Standard No. 75, Protection of Electronic Computer/Data Processing Equipment.

q. Naval Ships' Technical Manual, Chapter 631, Section 10.

r. United States Department of State, System Security Standard Number 2, Security Standards for Classified Automated Information Systems in the United States, October 1985.

s. United States Department of State, System Security Standard Number 3, Security Standards for Unclassified Automated Information Systems at Foreign Service Posts, May 1985.

t. United States Department of State, System Security Standard Number 5, Security Standards for Unclassified Automated Information Systems Connectivity World Wide, June, 1987.

u. Computer Fraud and Abuse Act of 1986 (Public Law 99-474)

v. Public Law 100-235, Computer Security Act of 1987, January 8, 1988

RIS: CS 1600-28

U.S. Department of Transportation
Federal Aviation Administration

SHORT FORM RISK ASSESSMENT

A risk assessment shall be conducted on all information systems, particularly sensitive information systems. This risk assessment is suitable for AIS risk analysis for the personnel computer environment, office automation networks and other small office systems, categorized as Office Automation (OA) Systems. It may also be used for mainframe systems, however, it is limited in when assessing these systems. It is not all inclusive and should be used only as a guide. It is intended to be a supplemental tool to your AIS security program and not to be used as the sole element to determine the security posture of the AIS. This form may also be used as a security profile for OA systems.

1. Activity/Organization	**2. Location of Equipment**
3. Person Assigned AISSO Respons. for System and Data	**4. Facility AIS Security Manager (AISSM)**
Name	Name
Title Routing Symbol	Title Routing Symbol
Telephone Number	Telephone Number

5. Identification of System: List all equipment and peripheral devices that are used on the system.

Equipment	Manufacturer	Model #	Serial #
A.			
B.			
C.			
D.			
E.			

6. How will the system be configured? (Check appropriate box)

□ A. Stand Alone

□ B. Stand Alone System with remote capability.

System you will access ____________________

Percentage of use as remote ____________________

□ C. Remote Terminal

□ D. Other (explain) ____________________

7. Who is the owner of the system?

□ A. U.S. Government

□ B. Contractor (list organization) ____________________

□ C. Privately owned (list name) ____________________

8. Total Dollar Value of System	**9. How many hours/day will system be used?**	**10. How many days per week?**

11. Will the system be processing classified information?

□ Yes □ No

If YES, then what level? □ Confidential □ Secret □ Top Secret □ Other ____________________

12. System Users

13. Do the individuals identified in Question 12 participate in an approved Personnel Security Program? □ Yes □ No

Explain Program

14. In the following chart, annotate as a percentage in the appropriate processing category, how the specific information is processed on the system (based upon the total hours used) during a normal work week.

	Processing/Storage Categories						
				Unclassified			
Type of Information	Top Secret	Secret	Confidential	PA	FOUO	SENS	NON
a. Personnel							
b. Inventory							
c. Financial/Budget							
d. Contractual							
e. Management Info							
f. Engineering							
g. Administrative							
h. Word Processing							
i. Data Base Mgmt.							
j. Other							

PA - Privacy Act; FOUO - For Official Use Only; SENS - Sensitive; NON - Non Sensitive

15. This system has the capability of storing information on the following magnetic media (check all applicable items).

□ A. Floppy Disk
□ B. Fixed Hard Disk
□ C. Removable Hard Disk
□ D. Fixed Hard Card
□ E. Other magnetic media ______________________
____

16. The following threats and countermeasures apply to this data processing activity. Fill in the blank space for what your consider the risk to be either high, medium, or low. Circle or check the countermeasures that apply for each threat.

a. FIRE

Risk □ High □ Medium □ Low

Countermeasures:

□ 1. Sprinklers installed
□ 2. Halon installed
□ 3. Fire extinguishers
□ 4. Fire Bell available
□ 5. Smoke detectors installed
□ 6. Fire alarm
□ 7. Fire resistant material, Non Combustible
□ 8. Written Emergency Plan
□ 9. Other ______________________

b. POWER LOSS

Risk □ High □ Medium □ Low

Countermeasures:

□ 1. Back-up power available
□ 2. Nonvolatile memory
□ 3. Auto-restart
□ 4. Power surge protection exists
□ 5. Other ______________________

c. WATER DAMAGE

Risk □ High □ Medium □ Low

Countermeasures:

□ 1. Computer location is above grade
□ 2. Raised floor
□ 3. Humidity recording device or indicators installed
□ 4. Dry pipe sprinkler
□ 5. Waterproof covers for equipment
□ 6. Closed metal files and cabinets
□ 7. Other ______________________

d. LOSS OF DATA INTEGRITY

Risk □ High □ Medium □ Low

Countermeasures:

□ 1. Security procedures
□ 2. Operating procedures (Proper data entry and back-up procedures)
□ 3. Air conditioning
□ 4. Antistatic measures (use of spray chemicals, humidifiers, etc.)
□ 5. Other ______________________

e. ELECTRIC HAZARD

Risk □ High □ Medium □ Low

Countermeasures:

□ 1. Equipment is grounded
□ 2. Power off controls
□ 3. Fire extinguishers
□ 4. Auto Logging
□ 5. Other ______________________

(Local Reproduction Authorized)

f. UNAUTHORIZED USE OR MISUSE

Risk □ High □ Medium □ Low

Countermeasures:

□ 1. Password system established (check one)
□ System access □ File access
□ 2. Operating System security incorporated
□ 3. Visitor logs and escort procedures established
□ 4. Access rosters established
□ 5. Input/Output receipt system implemented
□ 6. End-of-day checkout procedures established
□ 7. Other ______________________________

g. PHYSICAL PENETRATION

Risk □ High □ Medium □ Low

Countermeasures:

□ 1. Cipher locks exist and control procedures have been written and implemented
□ 2. Personal recognition
□ 3. Security Awareness (indoctrination and annual training)
□ 4. Key control procedures exist
□ 5. Combination locks exits and procedures have been written and implemented
□ 6. Other ______________________________

17. Contingency Planning

Indicate which of the following applies by circling the appropriate letter. Use the space, in 19 below, to explain your response. Include the name and phone number of the individual responsible for the administration of the contingency plan.

□ **A. A contingency plan exists.**

Briefly outline the elements of the plan. Has the plan been tested? When?

□ **B. A contingency plan is being discussed.**

Briefly explain at what state of development it is at and what remains to be done.

□ **C. To date no action has been taken to develop a contingency**

Please explain.

□ **D. A contingency plan is not required.**

Please explain in detail the conditions that make a contingency plan unnecessary. Indicate the name and position of the individual making this determination.

18. Inventory Control

□ A. Has the equipment been entered into the System Inventory Directory (SID) maintained by AMS-300?
□ Yes □ No

□ B. Has the equipment been entered in the Personnel Property Management Information System (PPMIS)?
□ Yes □ No

19. Remarks/Comments

20. Name and signature of individual preparing this form

Signature	Typed Name	Date	Routing Symbol

APPENDIX 4. CONTINGENCY PLAN FOR ARTCC

CHAPTER 1. - PRELIMINARY PLANNING

1. PURPOSE. This document establishes procedures for the operation of the ______________ ARTCC NAS Automation System in the event of a disaster or disruption to service. Air route traffic control centers (ARTCC) control all en route aircraft in the United States which are operating under instrument flight rules and are not under the control of the military or other facilities. The centers provide separation service, traffic advisories, and weather information to pilots while they are en route between airports.

2. SCOPE. The contingency plan is a document designed to be used in the event of an emergency. This plan is applicable to the present IBM 9020 computer system in operation to support air traffic control (ATC). The FAA has developed a replacement of the 9020 central computer complex with a host computer. This host computer will be capable of running the present 9020 software package with minimal modifications. This will allow for this contingency plan to be applicable with only minor revisions.

3. BACKGROUND. An ARTCC represents a unique data processing environment which does not allow for normal contingency planning as outlined in directives such as FIPS PUB 87. An individual ARTCC processes unique radar and flight data, which will not allow for operations to be processed at a back-up site or alternate center. All ARTCC's have redundancy built into the NAS system by design. These systems each have a back-up on line processor and have a third system available, the Direct Access Radar Channel (DARC) System. This system looks and functions in a similar manner to the prime channel computer. DARC will provide tracking, mosaicking, and real-time quality control and will allow each controller to select either mode of operation, prime channel computer, or DARC. If the prime channel computer becomes nonoperational, DARC will continue to track and display full data blocks.

4. ASSUMPTIONS. It is neither cost-effective nor prudent management practice to reduce every risk to zero probability or zero loss expectancy. Accordingly, realistic risk management, and contingency planning requires that plans be developed based on several categories of assumptions. The whole list of assumptions for inclusion in the document cannot be completed until well into the planning cycle. However, the following shall be included in the set of assumptions:

a. Nature of the Problem - It is necessary to plan for the general nature and range of events in a variety of environments. Each assumption should be viewed in terms of probability, scope, and feasibility to warrant consideration in the plan.

(1) NAS automation/processing equipment malfunctions or damage cause hardware systems to be partially or totally inoperable for extended periods of time.

(2) Damage or destruction of NAS automation data programs or procedural documentation prevent operation.

(3) Access is denied to the NAS automation facilities as a result of vandalism, bomb threats, labor disputes, acts of nature, fire, water damage, electrical outages, excessive heat or cold, or similar factors.

(4) "Emergency Operations Plan" are initiated that cause normal workload to be totally or partially replaced by special requirements.

(5) Limited or general war, insurrections, or similar conditions require the facility to assume a wartime/military mission.

(6) War, insurrections, or similar conditions results in destruction of the NAS computer facilities.

(7) Contractor operated equipment or facilities fail to maintain continuity of operations.

b. Priorities. Air Traffic (AT) and Airways Facilities (AF) management have a critical need to understand the manner in which priorities are determined. Therefore, predefined responsibilities and procedures for the recovery of the NAS Automation System are essential.

c. Commitments to or Assumptions of Support. Upon examination of the NAS Automation System, it is evident that recovery from any but minor problems usually requires action from overlapping areas of AT/AF management. The assumption of such support including letters of agreement, operational orders, and related matters should be addressed. The areas that should be addressed include the following:

(1) Availability of people of all categories; i.e. watch schedules and shift assignments.

(2) Availability of NAS automation equipment and support.

(3) Responsibilities for the joint, AT/AF operation of the NAS Automation System.

(4) Response of public utilities.

5. RESPONSIBILITIES. The automation specialist (AUS), systems engineer (SE), and computer operator (CO) shall function as a team to make decisions and provide the most efficient operation of the NAS automation program and equipment. The responsibilities and duties set forth in this document shall serve as a guide to overall contingency planning.

a. Automation Specialist (AUS). An AUS shall be assigned the overall responsibility for the operation of the NAS Automation System Program in support of the ongoing ATC. The specialist represents the area manager in-charge (AMIC) in matters concerning automation. As such, the AUS shall be responsible for matters concerning automation system performance is acceptable for Air Traffic Control (ATC) purpose.

b. Systems Engineer (SE). The Systems Engineer represents the top level of technical management during any 8-hour watch with the responsibility of directing all of the maintenance and NAS activities at the ARTCC. The engineer serves in the same capacity for AF as the AMIC for AT. The engineer and the AMIC shall coordinate any action prior to a system change initiation which could result in system loss or degradation.

c. Computer Operator (CO). The Computer Operator is responsible for implementing necessary commands to the NAS System as directed by the SE or the AUS. It is evident that there are overlapping areas of AT/AF responsibilities and procedures. It is mandatory that the representatives from AT and AF function as a team to provide support for this contingency plan.

6. STRATEGY. Since a contingency plan is designed to be used in the event of an emergency, it should contain all of the basic information required to identify actions necessary to protect the resources of the NAS Automation System. In addition, because the destruction of the entire NAS system is a possible scenario, copies of the contingency plan should be stored off-site similar to system backup tapes.

a. The contingency plan requires the following major elements:

(1) Emergency Response - Minimize the injury to personnel and damage to equipment and facilities.

(2) Backup Operations - permits as much of normal operations as is possible to be implemented with whatever resources available.

(3) Recovery Actions - permits expeditious and cost-effective recovery of full operations to take place.

b. Each of these elements will be discussed in greater detail in part three of the plan.

7. RECORD OF CHANGES. An essential element of any volatile document, such as a contingency plan, is a method of preparing, posting, and recording changes to the document. The SE will be the final approving authority to any changes to the contingency plan. Table 1-1 shall be used to record all changes or updates to the plan. Once documented, the plan provides a significant amount of information about an ARTCC and the NAS Automation System. If the plan is misused or compromised, it could result in considerable damage to the center or could result in severe impact to the NAS system. Consequently, the plan should be made available to only those personnel affected by the plan. A sample distribution would be the AT and AF managers, systems engineer, automation specialist, and the area manager in-charge.

8. - 199. RESERVED.

CHAPTER 2. PREPARATORY ACTIONS

200. PEOPLE. A key element to implementing an effective contingency plan is people. Skilled user and system personnel are required for the operation of the NAS Automation System. In order to provide the information required for varying degrees of emergencies, the contingency plan must incorporate the personnel required to operate the system at various levels into the facilities organization. The personnel sections of the plan should be updated whenever key personnel change positions.

a. A contingency plan should identify three to five members for each of the following operations teams:

(1) Emergency Response Team

(2) Backup Operations Team

(3) Recovery Operations Team

b. An individual may be a member of more than one team. Teams may be staffed on a rotating basis by PGM support and adaptation. The following information should be identified and included in the contingency plan for each member:

(1) Name

(2) Routing symbol

(3) Position

(4) Abbreviation

(5) Home and work phone number

(6) Contingency plan position

(7) Security clearance level

c. In addition to this personnel information, the plan should also contain the following information for each responsibility:

(1) Team responsibility

(2) Person primarily assigned, routing symbol, position

(3) Person alternatively assigned, routing symbol, position

(4) Summary of significant responsibilities

(5) Security clearance required

d. The purpose of this information is to ensure that critical personnel are available as required to accomplish emergency, backup, and recovery operations functions.

201. DATA: The dependence of the NAS Automation System on prompt recovery of operations after the accidental or intentional loss of data is so critical that even a few minutes with a loss of data can have serious consequences. Therefore, the contingency plan must accommodate needs for prompt:

a. Data Recovery Procedures

b. Adaptation Rebuilds

c. Data Base Currency

202. SOFTWARE: For the purpose of this contingency plan, the term "software" includes both system and applications software, and any local patches or adaptations to the system. Because of the expense involved in the development of software, it is one of the NAS system's most valuable resources. Therefore, exact inventories of software, to include national and local patches, shall be maintained on site with a complete set of backup tapes restored at a remote location.

a. It is imperative that the contingency plan contain:

(1) The name and location of off-site storage facility

(2) The point of contact and telephone number at off-site storage facility.

(3) An exact inventory of the materials stored at the off-site storage facility including program/application name, revision date, and media type.

b. In addition to these types of information, a detailed inventory of all applications should be maintained. As a minimum, this inventory should contain:

(1) NAS documentation

(2) Master and updated system programs

(3) Administrative programs

(4) Identification and documentation of national system

(5) Data base patches for interim problems

(6) Dated and current national and local patches

(7) Security requirement

c. Because of the importance of this type of information, and the value of the applications, this information should be continually updated as new applications and local adaptations are added to the system. In addition, it should be comprehensively analyzed periodically to ensure the information contained is accurate.

203. HARDWARE: Definitive inventories of all NAS Automation System hardware is an integral part of the contingency plan. This information is required to determine the level of backup operations possible and to provide the recovery team with necessary information to obtain replacement hardware and reconfigure the system and restore operations. The major function of this hardware information is to permit the partial or total replacement of NAS system hardware. Location and availability of replacement equipment should be ascertained from an inventory of on-site spares or procured from the FAA Depot at FAA Aeronautical Center or the FAA Technical Center.

204. COMMUNICATIONS: NAS communication requirements encompass extensive capabilities for processing data communications with external facilities and Government agencies. The contingency plan should provide maintenance control coordinators to serve as the monitor and control point for the data multiplexing and RCL networks, during emergency situations, as well as performing restoral switching.

205. SPACE: The provision of space into which the NAS Automation System can be placed after loss of an original site should be considered for two purposes, as follows:

a. Space which can be used temporarily while the original site is being rehabilitated.

b. Space into which the NAS Automation System can relocate with relative permanence, within the air traffic control facility.

206. POWER AND ENVIRONMENTAL CONTROLS: All ARTCC's have installed systems which employ Uninterruptable Power Supply (UPS). These systems provide protection against power line transients and provide a short period, following a primary power failure, to allow for standby diesel generators to be brought into operation to support the NAS Automation System. This transaction will occur and be transparent to the operation of air traffic control.

a. The effective and efficient operation of the NAS Automation System is directly related to dependable and adequate heating, ventilating, air conditioning (HVAC) systems and uninterruptable electrical power which ensures maximum availability of services.

b. The contingency plan shall include provisions for effective restoration of service in the event of:

(1) Unanticipated loss of public utilities

c. Depending on the severity of an incident, implement NAS backup/recovery plans.

d. Inform the Recovery Operations Team of system status so that operations may be resumed onsite as soon as possible.

e. Confirm the damage to the site and estimate the impact on systems and operations.

f. Select the proper actions to ensure the speedy restoration of the highest level of operations possible

306. RECOVERY OPERATIONS. The objective of the Recovery Operations section is to describe what to do in effecting recovery from the situations documented in the problem scenarios. The ultimate goal of recovery operations is to facilitate the rapid restoration of the data processing activity. That is, to achieve system recovery in a timely and cost-effective manner while minimizing adverse impacts to the system.

307. RECOVERY OPERATIONS TEAM. The goal of this team is to bring the system up to normal operations in a expeditious and cost-effective manner. Close coordination must be maintained with the Backup Operations Team.

APPENDIX 5. SUBJECT INDEX